

مقدمة قصيرة جدًّا

# الأعداد

بيتر إم هيجنز

# الأعداد

# الأعداد

## مقدمة قصيرة جدًّا

**تأليف**
**بيتر إم هيجنز**

ترجمة
أحمد شكل

مراجعة
إيمان عبد الغني نجم

مراجعة علمية
أ.د. انتصارات محمد حسن الشبكي



# الأعداد

بيتر إم هيجنز

# Numbers

Peter M. Higgins

**الطبعة الأولى ٢٠١٧م**
رقم إيداع ٢٦٧٢١ / ٢٠١٤


**مؤسسة هنداوي للتعليم والثقافة**
إن مؤسسة هنداوي للتعليم والثقافة غير مسئولة عن آراء المؤلف وأفكاره
وإنما يعبِّر الكتاب عن آراء مؤلفه
٥٤ عمارات الفتح، حي السفارات، مدينة نصر ١١٤٧١، القاهرة
جمهورية مصر العربية
**تليفون:** ٢٠٢ ٢٢٧٠٦٣٥٢ + **فاكس:** ٢٠٢ ٣٥٣٦٥٨٥٣ +
**البريد الإلكتروني:** hindawi@hindawi.org
**الموقع الإلكتروني:** http://www.hindawi.org

هيجنز، بيتر إم.
الأعداد: مقدمة قصيرة جدًّا/تأليف بيتر إم هيجنز.
تدمك: ٩٧٨ ٩٧٧ ٧٦٨ ٢٤٣ ٥

١-الرمزية في الأعداد
٢-الأعداد (رمزية)

أ-العنوان

٥١١,٣

تصميم الغلاف: إيهاب سالم.

# المحتويات

# تمهيد

إن الهدف من هذا الكتاب الموجز هو توضيح أنواع الأعداد المختلفة والأساليب التي تنتهجها بلغةٍ مألوفةٍ للجميع. تسمح الأعداد بإجراء المقارنات بين كل أنواع الأشياء، وأيُّ شخص لا يفهم الأعداد سيواجِه صعوباتٍ في العالم الحديث؛ إذ إن الأشياء التي يُعبَّر عنها عدديًّا موجودة في كل مكانٍ حولنا. مع ذلك ينبغي أن ندرك أن الأعداد — مع اعتيادنا عليها — ليس لها وجود ماديٌ، ولكنها كيانات مجردة نستنبطها من العالم الذي نعيش فيه. ولتكوين صورةٍ واضحةٍ عن كيفية استخداماتها، من الأفضل دراستها في حد ذاتها دون الإشارة إلى أي شيءٍ آخر.

هذا الكتاب الموجز ليس دورة تعليمية لتجديد المعلومات في علم الحساب، ولن نفرِط في تناول تاريخ نظام الأعداد؛ بل إن الغرض منه هو شرح الأعداد نفسها والأساليب التي تنتهجها. وبإلقاء نظرةٍ على جدول المحتويات، حيث توجد عناوين فصول الكتاب، ستجد أن الجزء الأول منه يتعامل على نحوٍ رئيسيٍّ مع أعداد العد المعتادة، بينما نتجاوزها في النصف الثاني؛ فمن خلال استكشاف المشكلات الطبيعية التي تظهر في المعاملات الجارية والعلوم، أخذَتْنا الحاجة إلى إجراء الحسابات دون قيود — في النهاية وبالتدريج — إلى ميدان الأعداد المركبة التي تُمثِّل إطار العمل الرئيسي لمعظم الأمور الخاصة بالأعداد. ربما يبدو الوضع مُقلقًا، ولكن اطمئِن؛ فقد تم الانتهاء بالفعل من الجزء الأصعب من العمل.

لم يأتِنا نظام الأعداد الحديث جاهزًا، وإنما تطوَّر على مدار قرونٍ عديدة. ومرَّت به فترات طويلة من التشوُّش الذي كان له مصدران: أولهما هو الافتقار لطريقةٍ فعالةٍ لتمثيل الأعداد التي نحتاجها؛ طريقةٍ تتيح لنا التعامل مع الأعداد. أما الثاني — الذي كان مرتبطًا بالأول — فكان شديد الصعوبة من الناحية الفلسفية فيما يتعلق بتفسيرات أنواع الأعداد المختلفة، وما إذا كانت ذات معنًى أم لا. وإننا لنشعر في الوقت الراهن بمزيدٍ من

الثقة بأنفسنا عندما يتعلق الأمر بما نحتاج — وما لا نحتاج — إلى أن نقلق حياله عند التعامل مع الأعداد؛ مما يجعل من الممكن تقديم صورة كاملة عن عالم الأعداد في كتابٍ واحدٍ موجزٍ مثل هذا الكتاب. هذا لا يعني أن كل الألغاز قد حُلَّت؛ بل الأمر بعيد عن ذلك كلَّ البعد، كما ستكتشف حينما تقرأ الكتاب.

بيتر إم هيجنز
كولشيستر، إنجلترا، ٢٠١١

الفصل الأول

# كيف لا تفكِّر في الأعداد؟

إننا معتادون جميعًا على رؤية الأعداد مكتوبة، وعلى استقاء معنًى منها. مع ذلك فالرقم 6 والعدد الذي يمثله الرقم ليسا الشيء نفسه. فعلى سبيل المثال، في الأرقام الرومانية نكتب الرقم 6 بهذه الطريقة: VI، ولكننا نعلم أن هذا يشير إلى نفس العدد الذي يُكتب 6 في الترقيم الحديث. ويشير الرمزان كلاهما إلى مجموعةٍ من الأشياء تتوافق مع علامات العد الست: I I I I I I. ولسوف نقضي بعض الوقت أولًا في دراسة الطرق المختلفة التي نستخدمها للتعبير عن الأعداد والتفكير فيها.

أحيانًا نحل المشكلات المنطوية على أعدادٍ دون إدراكٍ منَّا بحلها. على سبيل المثال، تصوَّر أنك تعقد اجتماعًا وترغب في ضمان حصول كل شخصٍ من الحضور على نسخةٍ من جدول الأعمال. يمكنك التعامل مع هذا الأمر عن طريق كتابة الحروف الأُولى من اسم كل شخصٍ سيحضر على نُسَخ الجدول، واحدةً تلو الأخرى. وما لم تنفد النسخ منك قبل أن تنتهي من هذه العملية فستعلم أن لديك عددًا كافيًا من النسخ لجميع الحضور؛ وبذلك تكون قد حللْتَ هذه المشكلة دون اللجوء إلى الحساب ودون العد المباشر على الرغم من اشتمال هذه العملية على الأعداد. فالأعداد تتيح لنا المقارنة الدقيقة بين مجموعةٍ وأخرى، حتى وإن كانت العناصر المكوِّنة للمجموعتين ذات طبيعةٍ مختلفةٍ تمامًا، كما هي الحال هنا؛ إذ تتكون إحدى المجموعتين من أشخاصٍ، بينما تتكون الأخرى من مجموعةٍ من الأوراق. إنَّ ما تسمح لنا الأعداد بالقيام به هو مقارنة الحجم النسبي لمجموعةٍ بالحجم النسبي لأخرى.

في السيناريو السابق لم تكن بحاجةٍ لحساب عدد الحضور؛ ولم تكن مضطرًّا لمعرفته، كانت مشكلتك هي تحديد ما إذا كان عدد نسخ جدول الأعمال يساوي على الأقل عدد الأشخاص، ولم تكن هناك حاجة لمعرفة قيمة هذين العددين. مع ذلك ستحتاج

إلى حساب عدد الحاضرين عندما تطلب غداءً لخمسة عشر شخصًا، وبالتأكيد عندما يتعلق الأمر بحساب فاتورة هذه الوجبة؛ فسوف يستخدم شخصٌ ما الحساب للتوصُّل إلى التكلفة الدقيقة، حتى لو أُجريت الحسابات جميعها على الآلة الحاسبة.

يسمح لنا نظام الأعداد الحديث بالتعبير عن الأعداد بطريقةٍ فعالةٍ ومنتظمةٍ دون تغيُّر، تجعل من السهل مقارنة عددٍ بآخر، وإجراء العمليات الحسابية التي تنشأ الحاجة إليها من خلال العد. إننا نستخدم يوميًّا نظام العد العشري لكل عملياتنا الحسابية — أي إننا نعد بالعشرات — ونفعل ذلك لسببٍ من قبيل المصادفة، وهو أن لدينا عشر أصابع في أيدينا. مع ذلك، ليس اختيارنا للنظام العشري هو ما يجعل نظام الأعداد لدينا فعالًا لهذه الدرجة، ولكن السبب هو استخدام القيمة المكانية في تمثيلات الأعداد؛ حيث تعتمد قيمة الرقم على مكانه في سلسلة الأعداد. على سبيل المثال، العدد 1984 هو اختصار للقيمة: 4 آحاد و8 عشرات و9 مئات وألف واحد.

من المهم أن نفهم ما نعنيه عند كتابة الأعداد بطرقٍ معينة. وسوف نتأمل في هذا الفصل ما تمثله الأعداد، ونستكشف طرق العد المختلفة، ونتعرف على مجموعةٍ مهمةٍ للغاية من الأعداد (الأعداد الأولية) ونقدِّم بعض الحيل العددية البسيطة لإيجاد هذه الأعداد.

## كيف صُنفتْ نُظُم العد؟

يستحق الأمر استغراق بضع لحظاتٍ في إدراك وجود مرحلتين متمايزتين لعملية وضع نظام عدٍّ يعتمد — على سبيل المثال — على العشرات. إننا نفرض على الأطفال مهمتين أساسيتين؛ هما حفظ الحروف الأبجدية وتعلُّم كيفية العد. هاتان العمليتان متشابهتان ظاهريًّا، ولكن بينهما اختلافات جوهرية. تعتمد اللغة الإنجليزية على ستة وعشرين حرفًا أبجديًّا، وكل حرف — تقريبًا — يرتبط بصوتٍ نستخدمه لنطق الكلمات. على أية حال، من المؤكد أن اللغة الإنجليزية قد تطوَّرت بحيث يمكن كتابتها باستخدام مجموعةٍ من ستة وعشرين رمزًا. مع ذلك، لا يمكننا تأليف القواميس ما لم نضع الحروف الأبجدية في ترتيبٍ معين. لا يوجد ترتيب طبيعي بعينه، والترتيب الذي استقرَرْنا عليه ويُدرس بالمدارس في قالبٍ نغمي — وهو $a, b, c, d, \dots$ — يبدو اعتباطيًّا للغاية بالفعل. وممَّا لا شك فيه أن الحروف الأكثر استخدامًا بوجهٍ عامٍّ تقع في النصف الأول من الحروف الهجائية، ولكن ذلك مجرد قولٍ اعتباطيٍّ وليس قاعدة؛ إذ إن الحرفين الشائعَي الاستخدام $s$ و$t$ على

سبيل المثال يقعان في ترتيبٍ متأخر. أما أعداد العد، أو «الأعداد الطبيعية» كما يشار إليها، 1، 2، 3 … جاءت إلينا على النقيض بالترتيب التالي: على سبيل المثال، الرمز 3 يراد به الإشارة إلى العدد الذي يلي 2، وهكذا يجب وضعه بعده. وحتى عددٍ معينٍ، يمكننا أن نبتكر اسمًا جديدًا لكل عددٍ متتالٍ. مع ذلك، عاجلًا أو آجلًا، سنُضطر إلى الاستسلام والبدء في تجميع الأعداد في مجموعات لكي نتعامل مع المتتالية غير المتناهية. والتجميع بالعشرات هو المرحلة الأولى لابتكار نظامٍ عدديٍّ مقبول، وكان هذا الأمر شبه عالميٍّ على مرِّ التاريخ وعبر العالم.

مع ذلك، كان يوجد كثير من الاختلافات في التفاصيل؛ فالنظام الروماني يفضِّل الجمع بالخمسات إضافةً إلى الجمع بالعشرات، باستخدام رموزٍ خاصة — مثل V وL — للخمسة والخمسين على التوالي. كان النظام الإغريقي يعتمد على التجميع بالعشرات، وكانوا يستخدمون حروفًا محددة للإشارة إلى الأرقام، وأحيانًا كانت تُميَّز بشَرطةٍ لتُعلم القارئ أن الرمز ينبغي قراءته على أنه رقم وليس حرفًا في كلمةٍ عادية. على سبيل المثال، الرمز $\pi$ يشير إلى 80 والرمز $\gamma$ يشير إلى 3؛ لذا ربما يكتبون $\pi\gamma$ لتعني 83. ربما يبدو ذلك مجديًا بالمثل، ويشبه بالفعل نظام الترقيم لدينا، ولكن الأمر ليس كذلك؛ فلم يصل الإغريق إلى فكرة النظام المكاني؛ إذ إن قيمة الرموز كانت ثابتة، فلا يزال الرمز $\gamma\pi$ يمثل نفس العدد 80 + 3، بينما إذا غيرنا ترتيب الخانات في 83، نحصل على العدد المختلف 38.

في النظام الهندي العربي تحققت المرحلة الثانية من التمثيل الرقمي. الفكرة الكبرى هنا هي جعْل قيمة الرمز تعتمد على مكان وقوعه على سلسلة الأعداد. وهذا يسمح لنا بالتعبير عن أي عددٍ بمجموعةٍ محددةٍ من الرموز. لقد استقرَرْنا على مجموعة الأرقام العشرة: 0، 1، 2، …، 9؛ لذا يُطلَق على النظام العددي العادي «نظام العد العشري»، ولكن كان يمكننا وضع نظامنا من مجموعةٍ أكبر أو أصغر من الرموز الأساسية. بل ويمكننا النجاح في ذلك باستخدام عددٍ قليلٍ من الأرقام يصل إلى رقمين، مثلًا 0 و1، وهو ما يُعرف باسم «النظام الثنائي»، الذي يُستخدم في أغلب الأحيان في الحوسبة. مع ذلك، لم يكن اختيار عدد رموز النظام هو العمل الثوري، وإنما الثوري هو فكرة استخدام المكان على السلسلة لتوصيل معلوماتٍ إضافيةٍ حول ماهية أعدادك.

على سبيل المثال، عندما نكتب عددًا على غرار 1905، فإن قيمة كل رقمٍ فيه تعتمد على مكانه على سلسلة الأعداد؛ فهنا يوجد 5 وحدات (آحاد) و9 وحدات من المئات (تمثل المائة $10 \times 10$)، ووحدة واحدة من الآلاف (يمثل الألف $10 \times 10 \times 10$). واستخدام رمز 0

مهم باعتبار أنه يشغل مكانًا على سلسلة الأعداد. ففي حالة 1905، لا تسهم خانة العشرات بشيء، ولكن لا يمكننا تجاهلها وكتابة الرقم 195؛ حيث إن هذا يمثل عددًا مختلفًا تمامًا. وبالفعل تُمثِّل كل سلسلةٍ من الأرقام عددًا مختلفًا، ولهذا السبب ربما تُمثَّل الأعداد الضخمة بسلاسل قصيرة؛ فيمكننا على سبيل المثال منْح عددٍ فريدٍ لكل إنسانٍ على الأرض باستخدام سلاسل لا تتكون من أكثر من عشرة أرقام، وبهذه الطريقة نقدم معرِّفًا شخصيًّا لكل فردٍ ينتمي إلى هذه المجموعة الضخمة.

كانت المجتمعات القديمة تستخدم أحيانًا أنظمة عدٍّ مختلفةً لكتابة الأعداد، ولكنَّ هذا أقل أهميةً من حقيقة أن جميعها تقريبًا افتقر إلى استخدام نظامٍ مكانيٍّ فعليٍّ في ظل استخدام الصفر استخدامًا غير منقوص باعتبار أنه يشغل مكانًا على سلسلة الأعداد. وبالنظر إلى مدى قدم حضارة بابل، فمن الرائع أن نجدهم من ضمن الشعوب القديمة التي اقتربت للغاية من التوصُّل إلى نظامٍ مكانيٍّ. مع ذلك، لم يستخدموا بالكامل الصفر كعدد — فهو ليس من بين الأعداد الطبيعية الخالصة — وتجنَّبوا استخدام الخانة الفارغة في المكان الأخير على السلسلة، بالطريقة التي نستخدمها لتمييز 830 عن 83 مثلًا.

كانت العقبة في المفهوم التي وجب إزالتها هي إدراك أن الصفر عدد بالفعل. ومما لا يمكن إنكاره أن الصفر ليس عددًا موجبًا ولكنه عدد بالرغم من ذلك، وسنظل نشعر بالعجز إلى أن نضعه ضمن نظامنا العددي على نحوٍ مناسب. ولقد اتُّخذت هذه الخطوة الحاسمة في الهند في زهاء القرن السادس الميلادي؛ ويطلق على نظامنا العددي «هندي عربي»؛ لأنه انتقل من الهند إلى أوروبا عن طريق جزيرة العرب.

## الحياة مع الكسور العشرية ودونها

استطعنا بالطبع الآن توسيع نطاق فكرة النظام العشري المكاني وألحقنا بها أجزاءً كسرية ليمثِّلا معًا نظام العد العشري المعروف. فعلى سبيل المثال، عندما نكتب 3.14، فإن الرقم 1 الذي يقع بعد الفاصلة العشرية يشير إلى وحدة واحدة من الكسر $\frac{1}{10}$؛ أي جزءًا من عشرة، وعلى نفس النحو تشير 4 إلى الكسر $\frac{4}{100}$. وهيئة العدد تلك، ذات المنزلتين العشريتين، مألوفة للغاية؛ حيث إننا نتعامل بالعملات العشرية التي لا يكون أصغر وحداتها الدولار أو الجنيه أو اليورو، باختلاف البلدان، وإنما البنس أو السنت، الذي يمثل جزءًا من مائة جزءٍ من وحدة العملة الرئيسية. والحساب العشري هو الامتداد الطبيعي لنظام العد العشري، ويُمثِّل تطبيقيًّا أفضل طريقةٍ لتنفيذ المسائل الحسابية

العادية. وعلى الرغم من مميزات هذا النظام، كانت نشأته بطيئة ومتردِّدة؛ فقد ظل محورَ اهتمام نخبة علماء الرياضيات فحسب، حتى أواخر القرن السادس عشر، حتى شق طريقه أخيرًا بدخول عالم الحسابات التجارية والاستخدامات العامة. وحتى بعد هذه الفترة استمرَّ التجميع اعتمادًا على أعدادٍ غير قوى العشرة. ولم تستخدم بريطانيا العملة العشرية حتى عام ١٩٧١، ولا يزال جزء من العالم المتحدِّث بالإنجليزية مصممًا على استخدام الياردات والأقدام والبوصات. دفاعًا عن وحدات القياس في النظام الملكي، فإنها مناسبة للقياس ومتوائمة تمامًا مع المقياس البشري للأشياء؛ فيبلغ طول كفِّ اليد من ستٍّ إلى ثماني بوصات، ويبلغ طولنا من خمسٍ إلى ست أقدام؛ لذا نحيط أنفسنا بأشياء من أحجامٍ متشابهة، تقاس بالفعل بوحدات البوصات والأقدام. مع ذلك، فتحديد عشر بوصات للقدم — بدلًا من اثنتي عشرة بوصة — كانت ستنجح أيضًا وكان سيسهُل التعامل معها عن طريق الآلات الحاسبة ذات النظام العشري.

إن عملية اتخاذ أساسٍ محددٍ لنظام العد تشبه قليلًا وضع مقياس رسمٍ شبكيٍّ محددٍ على خريطة؛ هذا الأساس ليس جزءًا جوهريًّا في النظام، ولكنه — بالأحرى — يشبه نظام إحداثيات مفروضًا على النظام بوصفه أداةً للتحكم فيه؛ فاختيارنا للأساس اعتباطي في طبيعته، والاستخدام الحصري لأساس العشرة يقصر رؤيتنا على مجموعة أعداد العد: 1، 2، 3، 4 ... إلخ، غير أننا نستطيع أن نرى الأعداد على حقيقتها مباشرةً فقط بإزاحة الستار عن هذه الرؤية المقصورة؛ فعندما نذكر عددًا معينًا، دعنا نَقُلْ على سبيل المثال تسعة وأربعين، فإننا جميعًا نمتلك صورة ذهنية للعدد 9 والعدد 4. ولكن هذا غير منصف نوعًا ما للعدد المعني؛ إذ إننا نضع في اعتبارنا على الفور أن تسعة وأربعين تساوي $9 + (10 \times 4)$. ونظرًا لأن $1 + (12 \times 4) = 49$، فربما يكون من السهل التفكير فيه بهذه الطريقة، وبالفعل عندما يكون الأساس اثني عشر، سيُكتب عندها تسعة وأربعون بالشكل 41؛ حيث يشير العدد 4 الآن إلى 4 أضعاف 12. مع ذلك، فإنَّ ما يمنح العدد تسعة وأربعين سمته هو أنه يساوي حاصل ضرب $7 \times 7$، المعروف باسم مربع العدد 7. وهذا الجانب من شخصية العدد يتضح بالأساس 7، وعندها سيُمثَّل العدد تسعة وأربعون بهذا الشكل: 100، حيث يشير العدد 1 إلى حاصل ضرب $7 \times 7$ مرة واحدة.

نحن مخوَّلون بالقدر نفسه لاستخدام أساسٍ آخر لنظام العد لدينا، على غرار اثني عشر: استخدم شعب المايا أساس العشرين، واستخدم أهل بابل أساس الستين. وإلى حدٍّ ما، العدد 60 خيار جيد كأساسٍ للعد؛ إذ إن لهذا العدد الكثير من القواسم — أي الأعداد

التي يقبل العددُ القسمةَ عليها — فهو أصغر عددٍ قابلٍ للقسمة على كل الأعداد من 1 حتى 6. مع ذلك، للعدد 60 الكبير نسبيًّا نقطة ضعف، وهي أن استخدامه كأساسٍ سوف يتطلب توفير 60 رمزًا مختلفًا لتشير إلى كل عدد من الأعداد بدءًا من صفر وحتى تسعة وخمسين.

يصبح العدد «عاملًا» من عوامل عددٍ آخر إذا كان العدد الأول ينقسم على العدد الثاني لعددٍ تامٍّ من المرات. على سبيل المثال، العدد 6 عامل للعدد 42 لأن 7 × 6 = 42، ولكن العدد 8 ليس عاملًا للعدد 28؛ حيث إن العدد 8 يتكرر في العدد 28 ثلاث مرات ويتبقى 4. وامتلاك عدد كبير من العوامل سمة مفيدة لأساس نظام الأعداد لديك، وهذا ربما يكون السبب في كون الاثني عشر خيارًا أفضل على الأرجح من العشرة، كأساسٍ للأعداد؛ حيث إن العدد 12 لديه 1، 2، 3، 4، 6، 12 في قائمة عوامله، بينما يُقسَم العدد 10 فقط على 1، 2، 5، 10.

إن الفاعلية والألفة التامة مع نظام العد لدينا تغمرنا بثقةٍ زائفة، وتفرض علينا بعض القيود؛ إذ نشعر براحةٍ أكبر في التعامل مع عددٍ صحيح عنها في التعامل مع تعبيرٍ (أو مقدارٍ) حسابي. فعلى سبيل المثال، يقول الناس 5969 وليس 127 × 47، مع أن التعبيرين كليهما يُمثِّلان نفس الشيء. وفقط بعد أن نتوصَّل إلى الإجابة — 5969 — نشعر بأن لدينا العدد ويمكننا أن ننظر إليه. مع ذلك، يوجد بعض الخداع في ذلك؛ حيث إننا كتبنا العدد في صورة مجموعٍ من قوى العشرة. ويمكن الاستدلال على الشكل العام للعدد وسماته الأخرى على نحوٍ أكبر من الصيغة البديلة التي يقسَّم فيها الرقم إلى عوامل. وبالتأكيد هذه الصورة المعيارية — 5969 — تسمح بالفعل بمقارنتها المباشرة بالأعداد الأخرى المعبَّر عنها بالطريقة نفسها، ولكنها لا تكشف الطبيعة الكاملة للعدد. وسوف تتعرَّف في الفصل الرابع على سبب آخر لأفضلية صيغة العوامل على التمثيل بالأساس عشرة، الذي يُبقي العوامل الأساسية خفية.

إحدى الميزات التي تمتَّع بها القدماء عنَّا هي أنهم لم يقعوا أسرى لعقلية الأسلوب العشري. وعندما تعلَّق الأمر بأنماط الأعداد كان من الطبيعي أن يفكِّروا من ناحية السمات الهندسية الخاصة التي يتمتع أو لا يتمتع بها عدد معين. على سبيل المثال، العددان 10 و15 عددان مثلثيان، وهو شيء يظهر لنا من خلال مثلث قوارير البولينج الخشبية العشر، أو مثلث الكرات الحمراء الخمس عشرة في لعبة السنوكر. ولكنَّ هذا شيء لا يطرأ على الذهن من الشكل العشري الأساس لهذين العددين فحسب. ويمكننا استعادة الحرية التي

تمتع بها القدماء تلقائيًّا من خلال تنحية تحيزات النظام العشري لدينا وإخبار أنفسنا بأننا أحرار في التفكير في الأعداد بطرقٍ مختلفةٍ تمامًا.

بعد تحرير أنفسنا بهذه الطريقة، ربما نختار التركيز على تحليل العدد إلى عوامل؛ أي الطريقة التي يمكن من خلالها كتابة العدد كنتيجةٍ لأعدادٍ أصغر مضروبةٍ معًا. يكشف التحليل إلى عواملَ شيئًا من البنية الداخلية للعدد. إذا توقَّفنا عن عادة التفكير في الأعداد بوصفها ببساطةٍ أدواتٍ للعلم والتجارة، وقضينا بعض الوقت في دراستها لسماتها في حد ذاتها دون الإشارة إلى أي شيءٍ آخر، فستُكشف الكثير من الأمور التي لولا ذلك لظلَّت خفية. ويمكن لطبيعة الأعداد المنفردة أن تُظهر نفسها بأنماطٍ منظمةٍ في طبيعتها، بطرقٍ أكثر دقةً من مجرد المثلثات والمربعات، على غرار الرأس الحلزوني لنبات عباد الشمس، الذي يمثل ما يطلَق عليه «عدد فيبوناتشي»، الذي سنتعرف عليه في الفصل الخامس.

## نظرة على متتالية الأعداد الأوَّلية

أحد أوجه عظَمة الأعداد بديهي للغاية، حتى إنه يمكن إغفاله بسهولة؛ وهو أن كل عدد منها فريد؛ فكل عددٍ له بنيته الخاصة، شخصيته المستقلة إذا أحببت قَوْلَ ذلك، وشخصية كل عددٍ منفردٍ مهمة؛ لأنه عندما يظهر عدد معين فإن طبيعته لها آثار على بنية المجموعة التي يُستخدم لها هذا العدد. وكذلك توجد علاقات بين الأعداد تكشف عن نفسها عندما نُطبِّق العمليات الحسابية الأساسية، وهي الجمع والضرب. ومن الواضح أن أي عددٍ أكبر من 1 يمكن التعبير عنه بوصفه مجموع أعدادٍ أصغر. مع ذلك، عندما نبدأ في ضرب الأرقام معًا، سريعًا ما نلاحظ أن أعدادًا معينة لا تظهر أبدًا في نتيجة عملياتنا الحسابية. هذه الأعداد هي الأعداد الأوَّلية، وهي تمثل اللبِنات الأساسية للضرب.

العدد الأوَّلي هو عدد مثل 7 أو 23 أو 103، يكُون له عاملان فقط، وهما بالضرورة 1 والرقم نفسه. (يُستخدم مصطلح «القاسم» أيضًا كبديلٍ لمصطلح العامل.) أما العدد 1، فلا نعتبره عددًا أوَّليًّا؛ لأنه ليس له إلا عامل واحد فقط. إذن، أول عددٍ أوَّليٍّ هو 2، وهو العدد الأولي الزوجي الوحيد، والأعداد الثلاثة الفردية التالية له 3، 5، 7 أعداد أوَّلية. والأعداد الأكبر من 1 وليست أعدادًا أوَّلية يُطلق عليها «أعداد مركبة»؛ إذ إنها تتكوَّن من أعدادٍ أصغر. والعدد $2^2 = 2 \times 2 = 4$ هو أول عدد مركب؛ والعدد 9 هو العدد الفردي المركب الأول، و$3^2 = 9$ هو أيضًا عدد مربع. والعدد 6 الذي يساوي $3 \times 2$ هو أول عدد مركب حقًّا؛ حيث إنه يتكون من عاملين مختلفين أكبر من 1 ولكن أصغر من العدد نفسه،

بينما $2^3 = 8$ هو العدد المكعب الأول، وهي الكلمة التي تعني أن العدد يساوي عددًا مرفوعًا للقوة 3.

بعد الأعداد المكونة من رقم واحد، لدينا العدد المختار كأساس، $5 \times 2 = 10$، الذي مع ذلك يُعد فريدًا لكونه «مثلثيًّا»؛ حيث $4 + 3 + 2 + 1 = 10$ (تذكَّر قوارير البولينج). بعدها لدينا عددان أوليان توءمان هما 11 و13، وهما عددان فرديان متتابعان كلاهما أوَّلي، ويفصلهما العدد 12، الذي — على النقيض من حجمه — لديه الكثير من العوامل. وبالفعل، العدد 12 هو العدد الأول الذي يُطلق عليه «عدد زائد»؛ حيث إن مجموع عوامله الحقيقية التي هي أقل من العدد؛ بمعنى أنها لا تشتمل على العدد نفسه، يتخطى العدد نفسه: $16 = 6 + 4 + 3 + 2 + 1$. وربما يبدو العدد $7 \times 2 = 14$ غير مميَّز، ولكن للمفارقة، إذا كان العدد غير المميَّز هو الأول في عدم تميُّزه، فذلك يجعله مميَّزًا بالرغم من كل شيء. وفي العدد $5 \times 3 = 15$، لدينا عدد مثلثي آخر، وهو أول عدد فردي يكون ناتجًا لعاملين حقيقيين فقط. وبالطبع العدد $2^4 = 16$ ليس مجرد عدد مربع فحسب، ولكنه أول رقم مرفوع للقوة الرابعة (بعد 1)؛ مما يجعله مميَّزًا للغاية بالفعل. والعددان 17 و19 عددان أوليان توءمان آخران. وسوف أترك للقارئ التوصُّل إلى ملاحظاته الخاصة حول الطبيعة الغريبة للعددين 18 و20 وما بعدهما. ومع كل عددٍ يمكنك اكتشاف ما يجعل منك شخصًا شهيرًا.

وبالعودة إلى الأعداد الأوَّلية، إليك أول عشرين عددًا أوَّليًّا:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,$$

$$47, 53, 59, 61, 67, 71.$$

من الواضح أن الأعداد الأوَّلية تكثر في بداية متتالية الأعداد، ولا تُتاح إلا فرص قليلة للغاية لأنْ يكون للأعداد الصغيرة عوامل. وبعد ذلك تصبح الأعداد الأولية أكثر ندرة. على سبيل المثال، يوجد ثلاثة فقط من الأعداد الأوَّلية المتتالية: فالثلاثية 3، 5، 7 فريدة من نوعها؛ إذ إن كل عددٍ فرديٍّ ثالثٍ على سلسلة الأعداد هو من مضاعفات العدد 3، وبهذا لا يمكن أن يتكرر الأمر مرة أخرى. مع ذلك، فعملية ظهور الأعداد الأولية المتباعدة بطيئة إلى حدٍّ ما وغير منتظمة على نحوٍ مذهل. على سبيل المثال، لا تتضمن الثلاثينيات إلا عددين أوَّليين فحسب، وهما 31 و37، مع ذلك، بعد 100 مباشرة يوجد زوج متتالٍ من التوائم الأوَّلية هو (101، 103) و(107، 109).

كانت الأعداد الأوَّلية محطَّ إعجابٍ لآلاف السنين؛ لأنها لا تنفد أبدًا (ادِّعاء سوف نُبرِّره في الفصل التالي) مع أنها تظهر بين الأعداد الطبيعية بطريقةٍ عشوائيةٍ إلى حدٍّ ما. وهذا الجانب الغامض وغير المتوقَّع من طبيعتها تم استغلاله في التشفير الحديث من أجل حماية الاتصالات السرية على شبكة الإنترنت، وهو ما يُمثِّل موضوع الفصل الرابع.

## التحقُّق من أوَّلية العدد: اختبارات قابلية القِسمة

أبسط طريقةٍ لإيجاد كل الأعداد الأولية حتى عددٍ معينٍ — مثلًا 100 — هي كتابة كل الأعداد وشطب الأعداد المركبة. يُطلَق على الطريقة التقليدية المعتمِدة على هذه الفكرة «غربال إراتوستينس» وتطبَّق كما يلي: ابدأ برسم دائرة حول 2 ثم اشطب كل مضاعفات 2 (الأعداد الزوجية الأخرى) في قائمتك. بعد ذلك عُدْ إلى بداية القائمة وارسم دائرة حول أول عدد تقابله لم يُشطب (والذي سيكون 3) ثم اشطب كل مضاعفاته في بقية القائمة. ومن خلال تكرار هذه العملية بعددٍ كافٍ من المرات، سوف تظهر الأعداد الأولية، وهي الأعداد التي لم تُشطب، مع أن بعضها داخل دائرة، والبعض الآخر بلا دائرة. على سبيل المثال، يُبيِّن الشكل ١-١ طريقة الغربال حتى العدد 60.

كيف تعرف متى تتوقَّف عن الغربلة؟ عليك تكرار هذه العملية حتى ترسم دائرة حول عددٍ أكبر من الجذر التربيعي لأكبر رقم في قائمتك. على سبيل المثال، إذا كنت تغربل كل الأعداد حتى 120، فسيكون عليك أن تكرر عملية الغربلة لمضاعفات 2، 3، 5، 7، وعندما ترسم دائرة حول 11 يمكنك أن تتوقف؛ إذ إن $121 = 11^2$. عند هذه المرحلة ستكون قد رسمت دوائر حول الأعداد الأوَّلية حتى أول عددٍ أوليٍّ يتجاوز الجذر التربيعي لأكبر عدد لديك (120 في هذه الحالة) مع عدم المساس بالأعداد الأوَّلية الباقية. وكل الأعداد المركبة ستصبح مشطوبة الآن؛ حيث إن كلًّا منها مضاعف لواحد أو أكثر من الأعداد الأولية 2، 3، 5، 7.

ليس من العسير إدراك السبب في أن الجذر التربيعي لأكبر عددٍ $n$ في قائمتك يحدِّد عدد المرات التي يجب تكرار العملية بها. (عند تفسير خصائص الأعداد الاختيارية، منَح علماء الرياضيات أسماءً — في صورة رموز — للأعداد محل النقاش. وهذه الأسماء عادةً ما تكون أحرفًا صغيرة على غرار $m$ و$n$؛ وناتج العددين $m \times n$ عادةً ما يُكتب اختصارًا $mn$.) وأي عدد مركب $m$ في قائمةٍ سيكون لديه عامل أوَّلي، وأصغر عامل أوَّلي له يجب

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~

~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~

~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~

شكل ١-١: غربال الأعداد الأوَّلية: الأعداد الأوَّلية حتى 60 هي الأعداد التي لم تُشطب.

ألا يكون أكبر من الجذر التربيعي للعدد $n$؛ لأن حاصل ضرب عددين أو أكثر يتخطيان $\sqrt{n}$ يكون أكبر من $n$ (وكذلك أيضًا أكبر من $m$).

جانب آخر من مسألة أوَّلية العدد يتمثَّل فيما إذا كان عدد $n$ معين هو عددًا أوَّليًّا أم مركبًا. لتحديد ذلك يمكننا اختبار $n$ بالقسمة على كل رقمٍ أوليٍّ تباعًا حتى $\sqrt{n}$، وإذا تخطَّى العدد $n$ كل هذه الاختبارات فسيكون عددًا أوَّليًّا، وإلا فلن يكون أوَّليًّا. ولهذا السبب، من العملي أن تكون هناك طرق بسيطة لاختبار القسمة على الأعداد الأولية الصغيرة 2، 3، 5، 7 ... ويمكن تلبية هذه الحاجة بسهولة كما يلي.

من اليسير للغاية اختبار قابلية القسمة على 2 و5؛ إذ إن هذين العددين الأوَّليين هما العاملان الأوَّليان لأساس نظام العد العشري لدينا. وفي ضوء ذلك، كل ما عليك فعله هو التحقُّق من الخانة الأخيرة في العدد $n$ محل النقاش: يكون $n$ قابلًا للقسمة على 2 عندما يكون رقم خانة الآحاد زوجيًّا (أي 0، 2، 4، 6، 8)، ويكون العدد 5 من عوامل $n$، فقط إذا كان ينتهي بصفر أو 5. وبغض النظر عن عدد الخانات التي يتكون منها $n$، نحتاج فقط إلى التحقُّق من الخانة الأخيرة لتحديد ما إذا كان لدينا عدد من مضاعفات 2 أو 5. وبالنسبة إلى الأعداد الأوَّلية التي لا تنقسم على 10، علينا القيام بمزيدٍ من الإجراءات، ولكن توجد اختبارات بسيطة لقابلية القسمة تُعد أسرع بكثيرٍ من اللجوء إلى القيام بعملية القسمة بأكملها.

يكون العدد قابلًا للقسمة على 3، فقط إذا كان الأمر نفسه ينطبق على مجموع أرقام خاناته. على سبيل المثال، مجموع أرقام خانات العدد $n = 145,373,270,099,876,790$ هو 87 و$87 = 3 \times 29$؛ ومن ثَمَّ فإن $n$ في هذه الحالة

يقبل القسمة على 3. وبالطبع يمكننا تطبيق الاختبار على العدد 87 نفسه، وبالتأكيد يمكننا الاستمرار في الحصول على مجموع أرقام خانات الناتج في كل مرحلةٍ حتى تصبح النتيجة واضحة. والقيام بهذا الأمر على المثال المذكور يُنتج التسلسل التالي:

$$145,373,270,099,876,790 \longrightarrow 87 \longrightarrow 15 \longrightarrow 6 = 2 \times 3.$$

سترى أن كل اختبارات القسمة المذكورة هنا سريعة للغاية بحيث يمكنك التعامل مع أعدادٍ مكونةٍ من عشرات الخانات بسهولةٍ نسبيةٍ حتى لو كانت هذه الأعداد أكبر بمليارات المرات من أكبر عدد يمكن لآلتك الحاسبة التعامل معه.

اختِيرت الاختبارات المذكورة هنا لبقية الأعداد الأوَّلية حتى العدد 20 لأنها تنتمي جميعًا إلى النوع العام نفسه، ويسهل تطبيقها مع أن السبب وراء نجاحها ليس بهذه الدرجة من الوضوح. ومع أن التفسيرات ليست مذكورة هنا، فإن إيجاد الدلائل على صحتها ليس أمرًا صعبًا على نحوٍ خاص.

دعنا نبدأ باختبار القسمة لعددٍ ما $n$ على 7. ضاعِف الرقم الموجود في الخانة الأخيرة في العدد $n$ واطرح الناتج من العدد الباقي بعد حذف الخانة الأخيرة. سيكون العدد الجديد من مضاعفات العدد 7 عندما يكون العدد $n$ من مضاعفاته. نكرر هذه العملية حتى تصبح النتيجة واضحة. وكمثالٍ بسيط، دعنا نأخذ العدد $n = 3465$: ضعف 5 هو 10، لذا نطرح 10 من 346 لنحصل على 336؛ بعد ذلك نكرر العملية مرة أخرى، فنطرح ضعف 6، وهو 12 من 33 لنحصل على $21 = 3 \times 7$، ومن ثَمَّ فإن $n$ يقبل القسمة على 7. إذا كنت قد نسيت جدول الضرب للعدد 7، يمكننا مراجعته مرة أخرى: طرح 1 مرتين من 2 ينتج 0، وهو يقبل القسمة على 7، حيث $0 = \frac{0}{7}$. (كل عددٍ من هذه الأعداد صفر على عددٍ صحيح؛ إنما العكس، أي القسمة على صفر، هو ما ليس له معنًى.) حتى العدد المكوَّن من عشرات الملايين يمكن التعامل معه بسهولةٍ بهذه الطريقة. وفي هذا المثال والأمثلة التالية، نذكر ببساطةٍ العدد الناتج في كل مرحلةٍ من الخوارزمية، وهو الاسم الذي يُطلَق على العملية الآلية — مثل هذه العملية — التي تحل مسألة من نوعٍ محدد.

$$n = 27,916,924 \longrightarrow 2,791,684 \longrightarrow 279,160 \longrightarrow 27,916$$

$$\longrightarrow 2,779 \longrightarrow 259 \longrightarrow 7$$

وهكذا فإن $n$ يقبل القسمة على 7. وفي كل مرةٍ نطبق فيها دائرة التعليمات، نفقد على الأقل خانة واحدة؛ ومن ثَمَّ فإن عدد مرات تكرار العملية هو تقريبًا نفس عدد خانات العدد الذي بدأنا به.

ولاختبار ما إذا كان $n$ لديه عامل 11، اطرح الرقم الموجود في الخانة الأخيرة في $n$ من العدد المستقطَع المتبقي وكرِّر العملية. على سبيل المثال، العدد التالي من مضاعفات العدد 11 كما تشير طريقتنا:

$$4,959,746 \longrightarrow 495,968 \longrightarrow 49,588 \longrightarrow 4,950 \longrightarrow 495$$

$$\longrightarrow 44 = 4 \times 11.$$

وللتحقق من القابلية للقسمة على 13، أضفْ أربعة أضعاف رقم الخانة الأخيرة إلى العدد المستقطَع المتبقي وأكمل العملية كما في حالة 7 و11. مثلًا، اتَّضح أن العدد 13 من العوامل الأولية للعدد التالي:

$$11,264,331 \longrightarrow 1,126,437 \longrightarrow 112,671 \longrightarrow 11,271$$

$$\longrightarrow 1131 \longrightarrow 117 \longrightarrow 39 = 3 \times 13.$$

أما بالنسبة للعددين 17 و19، نطرح خمسة أضعاف الرقم الموجود في الخانة الأخيرة في حالة 17، ونضيف ضعفه عند اختبار ما إذا كان 19 أحد عوامل العدد، ومرة أخرى نطبق هذه الخطوة على العدد المستقطَع المتبقي، ونكرر العملية وفق ما يلزم. على سبيل المثال، نختبر قابلية العدد $18,905$ للقسمة على 17:

$$18,905 \longrightarrow 1,865 \longrightarrow 161 \longrightarrow 11$$

إذن، هو ليس من مضاعفات العدد 17، ولكن بالنسبة للعدد 19، يؤدي الاختبار إلى العكس:

$$18,905 \longrightarrow 1,900 = 100 \times 19.$$

وبامتلاكك هذه الترسانة من الاختبارات، يمكن بسهولة التحقق من أولية كل الأعداد حتى 500 (إذ إن $529 = 23^2$ يتخطى 500، وبذلك فإن 19 هو أكبر عامل أولي محتمل

تضعه في اعتبارك). على سبيل المثال، لحل هذه المسألة بالنسبة للعدد 247، نحتاج أن نتحقق من قابلية القسمة حتى العدد الأولي 13 (حيث إن مربع العدد الأولي التالي $289 = 17^2$، يتخطى 247). مع ذلك، من خلال تطبيق اختبار العدد الأولي 13، نتعرف من الخوارزمية $13 \rightarrow 52 = (28 + 24) \rightarrow 247$ أن لدينا عددًا من مضاعفات 13 وهو ($247 = 19 \times 13$).

يمكن أيضًا إجراء اختبارات القابلية للقسمة على الأعداد الأولية، وفي الوقت نفسه إتاحة إجراء اختبارات قابلية القسمة على الأعداد التي تمثل نواتج «غير مربعة» للأعداد الأولية (أي الأعداد التي لا تقبل القسمة على مربع أي عدد أولي) على غرار $7\times3\times2 = 42$. العدد $n$ هنا سيقبل القسمة على 42، عندما ينجح $n$ في اختبارات القسمة الثلاثة على 2، 3، 7. مع ذلك، فاختبارات الأعداد التي لها عوامل مربعة — على غرار $3^2 = 9$ — لم تظهر تلقائيًّا، مع أن $n$ في هذه الحالة تملك 9 من بين عواملها، فقط إذا كان 9 من عوامل العدد الناتج عن مجموع الأرقام الموجودة في خانات العدد $n$.

ربما تتساءل: بعد آلاف السنين، ألم يبتكر هؤلاء الرياضيون الأفذاذ طرقًا أفضل وأكثر تطورًا لاختبار أولية العدد؟ الإجابة هي: بلى. ففي عام ٢٠٠٢، اكتُشفَت طريقة أسرع نسبيًّا لاختبار ما إذا كان عددٌ ما أوليًّا أم لا. مع ذلك، لا يوفر «اختبار إيه كيه إس لأولية عددٍ ما» عمليةَ التحليل لعوامل إذا تصادف أن كان العدد مركبًا. فلا تزال مشكلة إيجاد العوامل الأولية لعددٍ ما — مع أنها قابلة للحل مبدئيًّا من خلال التجربة — تبدو عسيرةً عمليًّا بالنسبة للأعداد الصحيحة الكبيرة؛ ولهذا السبب شكَّلَت أساس الكثير من عمليات التشفير العادي على الإنترنت، وهو الموضوع الذي سنعود لمناقشته في الفصل الرابع. وقبل أن نفعل ذلك، ألقِ نظرة أكثر دقة في الفصلين التاليين على الأعداد الأولية وعملية التحليل لعوامل.

الفصل الثاني

# متتالية الأعداد الأوَّلية غير المتناهية

## كيف تنتمي الأعداد الأولية إلى أحجية الأعداد؟

كيف يمكن أن نتأكد من أن الأعداد الأولية لا تزداد ندرةً لتختفي في النهاية تمامًا؟ ربما تعتقد أنه بوجود أعدادٍ لا متناهية وإمكانية تقسيم كلٍّ منها إلى أعداد ناتجة عن الأعداد الأولية (أمرٌ سأوضِّحه بدقة أكبر في السطور التالية)، لا بد أن يوجد عددٌ لا متناهٍ من الأعداد الأولية للقيام بهذه الوظيفة. مع أن هذا الاستنتاج صحيح، فإنه لا يَنتج عن الملاحظة السابقة؛ إذ إننا إذا بدأْنا بمجموعة متناهية من الأعداد الأولية، فلن توجد نهاية لعدد الأعداد المختلفة التي يُمْكننا إنتاجها باستخدام هذه العوامل الأولية فحسب. في الواقع، توجد قوًى مختلفةٌ كثيرة ولا متناهية لأيِّ عدد أولي: على سبيل المثال، قوى العدد الأولي 2 هي 2، 4، 8، 16، 32، 64 ... لذا من المرجح أنه يوجد عدد متناهٍ من الأعداد الأولية فقط، وكل عدد هو ناتج لقوى هذه الأعداد الأولية. وأكثر من ذلك أننا لا نملك طريقة لإنتاج متتالية لا متناهية من الأعداد الأولية المختلفة بالطريقة التي نستطيع بها — على سبيل المثال — إنتاج أي عدد من مربعات أو مضاعفات عدد معين. عندما يتعلق الأمر بالأعداد الأولية، علينا أن نبحث عنها، إذن كيف يمكننا أن نتأكد من أنها لن تنتهي؟

سوف نتأكد جميعًا قبل نهاية هذا الفصل، ولكن سوف ألفت انتباهك أولًا إلى «نمط» واحد بسيط فيما بين الأعداد الأولية يستحق الملاحظة. كلُّ عدد أوليٍّ — بخلاف 2 و3 — يقع على أحد جانبي مضاعفات العدد 6. بعبارة أخرى، إنَّ أي عدد أولي بعد هذين العددين يتكون من الصيغة $6n \pm 1$ بالنسبة للعدد $n$. (تذكرْ أن $6n$ هي صيغة مختصرة للمعادلة $6 \times n$ والرمز المزدوج ± يعني زائد أو ناقص.) والسبب في ذلك يَسْهل تفسيره. كل عدد يمكن كتابته بالضبط بصيغة من ست صيغ هي: $6n$ أو $6n \pm 1$ أو

$6n \pm 2$ أو $6n + 3$؛ حيث إن كل عدد لا يبتعد أكثر من ثلاثة أماكن عن أحد مضاعفات العدد 6. على سبيل المثال، $17 = (6 \times 3) - 1$، $28 = (6 \times 5) - 2$، $57 = (6 \times 9) + 3$. وفي الواقع تَظهر الصيغ الست دوريًّا؛ بمعنى أنك إذا كتبت أي ستة أعداد متتالية، فسوف تظهر صيغة من الصيغ الست مرة واحدة فقط، وبعد ذلك سوف تُعاوِد الظهور مرة أخرى بالترتيب نفسه. من الواضح أن أعداد الصيغتين $6n$ و$6n \pm 2$ أعدادٌ زوجية، بينما أي عدد من الصيغة $6n + 3$ يقبل القسمة على 3. ومن ثم فإنه، باستثناء 2 و3، يمكن أن يكون عددا الصيغة $6n \pm 1$ فقط هما الأوليَّين. وتتوافق الحالة التي يكون فيها عددا الصيغة $6n \pm 1$ كلاهما عددَين أوليَّين مع عددين أوليَّين توءمين: على سبيل المثال $(6 \times 18) \pm 1$ تُنتج الزوج 107 و109 المذكورَين في الفصل الأول. وربما تَمِيل للظنِّ بأن أحد عددَي الصيغة $6n \pm 1$ «على الأقل» دائمًا ما يكون أوليًّا؛ وهذا صحيح بالتأكيد بالنسبة للأعداد الأولية أقل من 100، ولكن أول مخالفة لهذه القاعدة ليس بعيدًا عن ذلك بكثير: $19 \times 7 = 119 = (6 \times 20) - 1$، بينما $11^2 = 121 = (6 \times 20) + 1$؛ ومن ثم عندما تكُون $n = 20$، لا يكون أيٌّ من العددين أوليًّا.

والسبب الرئيسي في كَوْن الأعداد الأوليَّة مهمةً هو أنَّ كلَّ عدد يمكن أن يُكتب كناتج للأعداد الأولية، ويمكن القيام بذلك أساسيًّا بطريقة واحدة فقط. ولإيجاد عملية التحليل الخاصة للعوامل تلك، علينا تحليل العدد المعيَّن إلى عوامله بطريقة ما ونُواصل تحليل أيِّ عوامل مركبة تظهر حتى نصل لنقطةٍ لا يمكن فيها القيام بذلك. على سبيل المثال، يمكننا القول بأن $120 = 2 \times 60$ ونواصل بتحليل العامل المركب 60 لنصل إلى:

$$120 = 2 \times 60 = 2 \times (2 \times 30)$$

$$= 2 \times 2 \times 2 \times 3 \times 5.$$

وبذلك نقول إن عملية تحليل العدد 120 لعوامله الأولية هي $2^3 \times 3 \times 5$. مع ذلك، يمكننا الوصول إلى هذه النتيجة بطريقة أخرى. على سبيل المثال:

$$120 = 12 \times 10 = (3 \times 4) \times (2 \times 5) = (3 \times (2 \times 2)) \times (2 \times 5)$$

وبذلك فإن إعادة ترتيب العوامل الأولية من الأصغر إلى الأكبر لا تزال تؤدي للنتيجة السابقة نفسها: $120 = 2^3 \times 3 \times 5$.

على الأقل، حدث ذلك في هذا المثال، وهذا السلوك ربما يكون مألوفًا لك إلى حدٍّ ما، ولكن كيف يمكن أن تتأكد من أن ذلك ينطبق على كل عدد؟ من الجليِّ على نحو

كافٍ أن أيَّ عدد يمكن تحليله إلى ناتج من الأعداد الأولية، ولكن إذا كان يوجد أكثر من طريقة عمومًا للتعامل مع هذه المسألة، فكيف يمكن أن نتأكد من أن العملية ستصل للنتيجة النهائية نفسها؟ هذا سؤال مهم؛ لذا سأستغرق بضع لحظات في شرح الخطوط العريضة للمنطق الذي سيسمح لنا بالتأكد من ذلك تمامًا. إن هذا الأمر نتيجة لِسِمَة فريدة أخرى في الأعداد الأولية التي سنطلق عليها «الخاصية الإقليدية» إذا كان العدد الأولي عاملًا لناتجِ عددين أو أكثر، فإنه حينها عامِل لأحد هذين العددين المشتركين في إنتاج العدد. على سبيل المثال، 7 عامل في المعادلة $280 = 35 \times 8$ (حيث إن الناتج $40 \times 7 = 280$)، ونلاحظ أن 7 عاملٌ من عوامل 35. وهذه الخاصية تميِّز الأعداد الأولية؛ إذ لا يمكن للأعداد المركَّبة أن تَضْمن الأمر نفسه: على سبيل المثال، نعلم أن 6 عامل في معادلة $120 = 15 \times 8$ (حيث إن $20 \times 6 = 120$)، مع ذلك 6 ليس عاملًا من عوامل 8 أو 15.

يمكن إثبات حقيقة أنَّ الأعداد الأولية تمتلك الخاصية السابقة في جميع الأحوال من خلال استخدام برهان معتمِد على ما يطلَق عليه «خوارزمية إقليدس»، التي سنتناول شرحها في الفصل الرابع. إذا سلَّمْنا بصحتها في الوقت الراهن، فليس من الصعب توضيح سبب عدم إمكانية إجراء عمليتين مختلفتين للتحليل إلى العوامل الأولية لأيِّ عدد، بافتراض وجود مثل هذا العدد. فحينها سيسلك العدد الأصغر هذا السلوك، دعْنا نشير إليه بالرمز $n$؛ ومن ثم فإن $n$ سيتيح إجراء عمليتَيْ تحليل إلى عوامل أولية ستكونان غير متطابقتين عند كتابة العوامل الأولية بترتيب تصاعدي. سوف نبيِّن أن هذا يؤدي إلى تناقُض؛ ومن ثم فلا بد أنه خاطئ.

إذا كانت عمليتا تحليل العدد $n$ إلى عواملَ تشتركان في العدد الأوَّلي $p$، يمكننا إلغاء $p$ منهما والحصول على عمليتين مختلفتين للعدد الأصغر $\frac{n}{p}$. ولما كان $n$ هو العددَ الأصغر الذي تُجرى عليه عمليتا تحليل مختلفتان إلى عوامل أولية، فهذا ليس ممكنًا؛ وبهذا يجب ألا تتضمن كلُّ مجموعة من الأعداد الأولية الموجودة في عملية تحليل العدد $n$ إلى عوامل عددًا أوليًّا مشتركًا. والآن خذ أحد الأعداد الأولية $p$ الذي ظهر في إحدى عمليتَي تحليل العدد إلى عوامل. ولما كان هذا العدد الأوليُّ $p$ هو عاملًا من عوامل $n$، فإن ذلك يتبعه أن يكون $p$ عاملًا من عملية التحليل الثانية، وهكذا، عن طريق الخاصية الإقليدية، $p$ عاملٌ من عواملِ أحدِ الأعداد الأولية — $q$ على سبيل المثال — لعملية التحليل الثانية. ولكن لما كان $q$ و$p$ عددين أوليَّين، فإن هذا الأمر ممكن فقط إذا كان $q = p$،

وهي الإمكانية التي أسقطناها بالفعل؛ حيث إن عمليتَي تحليل العدد $n$ إلى عوامل، ليس بهما عدد أوليٌّ مشترك. وهكذا وصلنا لتناقُض أخير، موضِّحِين أنه من المستحيل وجود هذا العدد $n$. ومن ثم نستنتج أن عمليةَ التحليل إلى عوامل أولية لكلِّ عددٍ عمليةٌ فريدة لا مثيل لها.

من الجدير بالذكر أنَّ تميُّز عملية التحليل إلى عوامل أولية لن يستمر إذا تضمَّنَت الأعدادُ الأوليةُ العددَ 1؛ إذ يمكننا ضمُّ أيِّ قوة للعدد 1 إلى عملية التحليل، وسيبقى الناتج بقيمته نفسها. وهذا يبين أن 1 يختلف جذريًّا في طبيعته عن الأعداد الأولية؛ ومن ثم فمن الصحيح صياغةُ تعريفٍ للعدد الأولي بطريقة تَستبعد 1 من مجموعة الأعداد الأولية.

## عدم تناهي الأعداد الأولية لدى إقليدس

دعنا نَعُدْ للتساؤل عن كيفية معرفة أن الأعداد الأولية لا تنتهي، وأنها لا يتجاوزها شيء. إذا ادعى شخصٌ ما أن 101 هو أكبر الأعداد الأولية، يمكنك دحْض ادعائه على الفور بإيضاحِ أنَّ 103 ليس له عوامل (عدا 1 و103)؛ ومن ثم فإن 103 هو أكبر من 101 فيما بين الأعداد الأولية. حينئذٍ ربما يعترف صديقك أنه أخطأ وأنه كان ينبغي أن يقول إن 103 هو أكبر الأعداد الأولية. يمكنك حينها أن تبين له مرة أخرى أن 107 عدد أولي أيضًا، ولكن ربما يظل صديقك مصرًّا على خطئه عن طريق تعديل موقفه إلى أكبر عدد أولي تَذْكُرُه. وربما يمكن أن يتراجع قليلًا ويعترف أنه لا يعرف أكبر عدد أولي، ولكن يُصِرُّ مع ذلك على ادعاء تأكُّده من وجود هذا العدد.

أفضل طريقة لتسوية المسألة هي توضيح أنه في حالة وجود أي مجموعة متناهية من الأعداد الأولية، يمكننا تقديم عدد أولي جديد ليس موجودًا في القائمة. على سبيل المثال، إذا ادَّعى شخصٌ ما وجود أكبر عدد فردي في مكان ما، يمكنك دحض هذا الادعاء بقولك إنه إذا كان $n$ عددًا فرديًّا، فإن $n + 2$ عددٌ فردي أكبر منه؛ لذا لا يمكن أن يوجد أكبر عدد فردي. مع ذلك، هذه الطريقة ليست بهذه السهولة مع الأعداد الأولية؛ فعند وجود قائمة متناهية من الأعداد الأولية، لا تُتاح لنا طريقة لاستخدام المجموعة لإنتاج عدد أولي أكبر من المجموعة كلها إلى حدٍّ بعيد. ربما يوجد عدد أولي أكبر بالرغم من كل شيء. كيف يمكن أن نَعرِف أن صديقنا العنيد ليس محقًّا؟

عرَّف ذلك إقليدس — عالم الرياضيات الإغريقي الذي تُنسَب إليه كلُّ صُوَر الرياضيات الإقليدية — الذي عاش في الإسكندرية (زهاء ٣٠٠ قبل الميلاد). بافتراض وجود قائمة $p_1, p_2, \ldots, p_k$، حيث يشير كلٌّ $p_i$ إلى عدد أولي مختلف، لم يستطع إقليدس إيجاد طريقة لإنتاج عدد أولي جديد؛ لذا لجأ إلى برهانٍ أكثر دقة. فأوضح أنه لا بد من وجود عدد أولي جديد أو أكثر ضمن نطاق معين من الأعداد (ولكن حجته لم تُمَكِّنَّا من معرفة المكان المحدد الذي نجد فيه العدد الأولي في هذا النطاق).

يسير الأمر على المنوال التالي: لنفترض أن $p_1, p_2, \ldots, p_k$ هي قائمة الأعداد الأولية $k$ الأولى على سبيل المثال، ولنعتبِر العدد $n$ عددًا أكبر من ناتج كل هذه الأعداد الأولية، بحيث $n = p_1 p_2 \ldots p_k + 1$. إما أن $n$ عدد أولي وإما أنه عدد يقبل القسمة على عدد أولي أصغر منه لا يمكن أن يكون أيًّا من $p_1, p_2, \ldots, p_k$؛ إذ إنه إذا كان $p$ أيًّا من هذه الأعداد الأولية، فإنه بقسمة $n$ على $p$ سوف يتبقى 1. ومن ثم فإنَّ أيَّ عدد أولي يَقْبل العددُ $n$ القسمةَ عليه هو عددٌ أولي جديد أكبر من كل الأعداد الأولية في القائمة $p_1, p_2, \ldots, p_k$ ولا يزيد عن $n$ نفسه. وعلى نحو خاص، يَنتج عن هذا أنه لا يمكن وجود قائمة متناهية من الأعداد الأولية التي تتضمن كلَّ الأعداد الأولية، وهكذا تستمر متتاليةُ الأعداد الأولية للأبد ولن تنفد أبدًا. إن برهان إقليدس الخالد حوْل عدم تناهي الأعداد الأولية يُعَدُّ من بيْن أكثر الإثباتات الرياضية إثارةً للإعجاب.

على الرغم من أن برهان إقليدس لا يحدد بالضبط مكان وجود العدد الأولي التالي، فإن التكرار العام للأعداد الأولية مفهوم تمامًا في الوقت الراهن. على سبيل المثال، إذا أخذنا أي عددين — مثلًا $a$ و$b$ — ليس بينهما عاملٌ مشترك، ونَظَرْنا إلى المتتالية $a, a + b, a + 2b, a + 3b, \ldots$، فسنجد — كما أوضح عالم الرياضيات الألماني يوهان دركليه (١٨٠٥–١٨٥٩) — أن الكثير من حدود هذه المتتالية أعداد أولية بغير تناهٍ. (بالطبع لا يوجد أمل إذا كان العددان $a$ و$b$ بينهما بالفعل عامل مشترك $d$ — مثلًا — إذ يكون كلُّ حدٍّ من حدود المتتالية أيضًا من مضاعفات $d$؛ ومن ثم فإنه ليس عددًا أوليًّا.) عندما يكون $a = 1$ و$b = 2$، نحصل على متتالية الأعداد الفردية التي نَعْرف من خلال برهان إقليدس أنها تحتوي على عدد لا متناهٍ من الأعداد الأولية. وبالفعل من خلال تعديلات بسيطة إلى حدٍّ ما لبرهان إقليدس، يمكن توضيح أن الحالات الخاصة الأخرى على غرار متتالية الأعداد من صيغة $3 + 4n$ و$5 + 6n$ و$5 + 8n$ (حيث تمثل $n$ القيم المتتالية 1، 2، 3 ...) كلٌّ منها يمتلك عددًا لا متناهيًا من الأعداد الأولية. مع ذلك، فالنتيجة العامة لنظرية دركليه يصعُب إثباتها للغاية.

نتيجة أخرى يَسْهل استنباطها؛ هي أنه يوجد دائمًا عدد أولي واحد على الأقل أكبر من أي عدد $n$، ولكنه أقل من $2n$ (حيث $n \geq 2$). (فقط للتذكرة، علامة عدم التساوي على غرار هذه العلامة التي تعني أكبر من أو يساوي، دائمًا تشير نحو الكمية الأصغر.) وهذه الحقيقة — المعروفة تاريخيًّا باسم «فرضية برتراند» — يمكن إثباتها باستخدام الرياضيات البسيطة، مع أن البرهان في حد ذاته معقد بالفعل. فيمكننا إثبات صحة الفرضية للعدد $n$ حتى 4000 عن طريق استخدام قائمة الأعداد الأولية التالية. لاحظْ أولًا أن كلَّ عدد في القائمة بعد العدد الأولي 2 أصغر من ضعف العدد التالي له:

$$2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259, 2503, 4001.$$

لكل عدد $n$ في النطاق حتى 4000، خذ أكبر عدد أولي $p$ في القائمة، لا يزيد عن $n$؛ حينئذٍ سيقع العدد الأولي التالي $q$ ضمن النطاق $n < q < 2n$، وهذا يضمن أن فرضية برتراند تنطبق على كل $n$ حتى 4000. على سبيل المثال، عندما تكون $n = 100$، فإن $p = 83$؛ إذن $q = 163 < 2 \times 100$. وتوضح المبرهنة الدقيقة التي تتضمن حجمَ ما يطلَق عليه «معاملات ذات الحدَّين المركزية» (المشروحة في الفصل الخامس) أن الفرضية تنطبق أيضًا على $n$ أكبر من 4000.

مع ذلك، ليس علينا أن نذهب بعيدًا لكي نقابل مشكلات تبدو شبيهة بهذه ولم تُحَلَّ بعدُ. على سبيل المثال، لا أحدَ يَعْلم ما إذا كان يوجد دائمًا عدد أولي بين عددين مربعين متتابعين. وتوجد ملاحظة أخرى تشير إلى احتمالية وجود أعداد أولية كافية لضمان أن كلَّ عدد زوجي $n$ أكبر من 2 يمثل مجموع اثنين منهما (حدسية جولدباخ). ولقد أُثبتت هذه الحدسية للعدد $n$ حتى $10^{18}$. ربما نأمل إذن في برهان شبيه بالمذكور سابقٍ لفرضية برتراند؛ حيث نبين أنه بعد عدد صحيح معين $N$، ربما نقدم مقارنة معتمدة على ما هو معروف عن توزيع الأعداد الأولية لضمان أنه سيوجد دائمًا على الأقل حل واحد في الأعداد الأولية $p$ و$q$، للمعادلة $p + q = 2n$ لأي عدد زوجي $2n \geq N$. ولا يزال هذا بعيد المنال، مع أنه توجد نتائج أضعف خلال هذه السطور؛ فعلى سبيل المثال، من المعروف منذ عام ١٩٣٩ أن كل عدد فردي كبير هو مجموع ثلاثة أعداد أولية على الأكثر، وأن كل عدد زوجي هو مجموع ما لا يزيد عن ثلاثمائة ألف عدد أولي. ولا يزال الإثبات التام لحدسية جولدباخ بعيد المنال.

توجد نتيجة بسيطة تنطوي على ما يشبه برهانًا على ما سبق، وهي أنه يوجد عدد $n$ أقل من 4 مليارات يمكن كتابته كناتج لمجموع أربعة أعداد مكعبة مختلفة بعشر

طرق مختلفة. من المعروف أن $1729 = 1^3 + 12^3 = 9^3 + 10^3$ هو أصغر عدد ناتج عن جمع عددين مكعبين بطريقتين مختلفتين. مع ذلك، فليس علينا بالضرورة أن نحدد العدد $n$ لكي نعلم أنه لا بد من وجوده. أحيانًا من الممكن أن نعرف، على نحو مؤكد، أنه يوجد حلول لمسألةٍ ما بدون إيجاد أيٍّ من هذه الحلول بالفعل على نحو واضح.

في هذه الحالة نبدأ بملاحظة أنه إذا أخذنا أربعة أعداد مختلفة ليست أكبر من عدد صحيح ثابت $m$ ويمثل مجموع مكعباتهم، فإن الناتج سيكون أقل من $4m^3$. مع ذلك، إذا كان $m = 1000$، فإن الحساب البسيط سيوضح أن العدد الناتج من جمع أربعة مكعبات مختلفة أكبر من 10 أضعاف العدد $4m^3$؛ ومن ثم فإن عددًا ما $n \leq 4m^3 = 4,000,000,000$ يجب أن يكون ناتجَ مجموعِ أربعةِ مكعبات بعشر طرق مختلفة على الأقل. وتتضمن التفاصيل حسابات أُجريت باستخدام معاملات ذات الحدين (المشروحة في الفصل الخامس)، وليست صعبة على نحو خاص.

تتلخص الصورة الشاملة لتوزيع الأعداد الأولية في ملاحظات العالِم الألماني البارز — من القرن التاسع عشر — كارل فريدريك جاوس (١٧٧٧–١٨٥٥) في مجالَي الرياضيات والفيزياء بأن $p(n)$ — أي عدد الأعداد الأولية حتى العدد $n$ — يتحدد تقريبًا من خلال $n/\log n$، وأن هذه المقاربة تصبح أكثر دقة كلما زاد $n$. على سبيل المثال، إذا كان $n$ يساوي مليونًا، فإن نسبة $n/\log n$ تشير إلى أن حوالي عدد واحد ينبغي أن يكون أوليًّا من بين كل 12.7، حتى هذا المليون. ولم تُثبَت ملاحظة جاوس حتى عام ١٨٩٦، وهي تشير بالتفصيل لشيء أكثر دقة. والدالة اللوغاريتمية المُشار إليها هنا يُطلق عليها «اللوغاريتم الطبيعي»، ولا تعتمد على قوى 10، ولكن على قوى عدد خاص $e$، يساوي تقريبًا 2.718. ولسوف تقرأ المزيد عن العدد $e$ الشهير للغاية في الفصل السادس.

المسألة الأكثر شهرة التي لم تُحل بعدُ في نظرية الأعداد هي فرضية ريمان التي يمكن تفسيرها فقط من خلال الأعداد المركبة التي سوف نذكرها لاحقًا. مع ذلك ذكرتُها هنا؛ حيث يمكن إعادة صياغة محور المسألة بالاستفادة من تميُّز عملية التحليل إلى عوامل أولية؛ لتتضمن ناتجًا معينًا غير متناهٍ يَضمُّ كلَّ الأعداد الأولية. وهذا يؤدي إلى تفسير يقول إن الفرضية تشير ضمنًا إلى أن التوزيع العام للأعداد الأولية منتظم للغاية، لدرجة أنه على المدى الطويل سوف تَحدث أولية الأعداد عشوائيًّا على نحو ظاهري. بطبيعة الحال، كَوْنُ عددٍ معيَّنٍ أوليًّا أم لا ليس حدثًا عشوائيًّا، ولكن المقصود هو أن أولية العدد — على نطاق واسع جدًّا — ترتدي عباءة العشوائية، مع عدم ظهور نمط أو

بنية إضافية. ويأمل الكثير من منظِّري الأعداد من أعماق قلوبهم أن يروا هذه الحدسية البالغ عمرها مائة وخمسين سنة تُحل خلال حياتهم.

نظرًا لأن الأعداد الأولية تُمثِّل متتالية طبيعية للغاية، فلا يمكن مقاومة البحث عن أنماط فيما بينها. مع ذلك لا يوجد صِيَغٌ مفيدة حقًّا للأعداد الأولية؛ أي لا توجد قاعدة معروفة تسمح بإنتاج كل الأعداد الأولية أو حتى حساب متتالية تتكون بالكامل من أعداد أولية مختلفة. وتوجد بعض الصيغ الواضحة، ولكنها ليس لها قيمة عملية كبيرة، وبعضها يتطلب حتى معرفة بمتتالية الأعداد الأولية لحساب قيمتها؛ وبهذا فهي احتيال بصفة أساسية. فالتعبيرات الجبرية على غرار $n^2 + n + 41$ يطلق عليها «متعددة الحدود»، وهذه الصيغة مصدر غني على نحو خاص بالأعداد الأولية. فعلى سبيل المثال، عند وضع $n = 1$، و$n = 7$، و$n = 20$ تباعًا، فإن ذلك يُنتج الأعداد الأولية 43 و107 و461 على الترتيب. وفي الواقع، ناتج هذا التعبير الجبري يَكُون عددًا أوليًّا لكل قيم $n$ بدءًا من $n = 0$ حتى $n = 39$. مع ذلك، في الوقت ذاته سوف تخذلنا هذه الصيغة المتعددة الحدود عندما نضع قيمة $n = 41$؛ إذ إن 41 سيكون عاملًا من عوامل الناتج، وبالطبع ستخفق عند $n = 40$.

$$40^2+40+41=40(40+1)+41=40\times41+41=(40+1)41=41^2.$$

بوجه عام، من الأمانة توضيح أنه لا يوجد صيغة متعددة الحدود من هذا النوع يمكن أن تُنتج صيغة للأعداد الأولية، حتى لو وضعْنا قُوًى أعلى من 2 في التعبير الجبري.

من الممكن ابتكار اختبارات لأولية الأعداد يمكن صياغتها بكلمات قليلة. مع ذلك، لكي تكون الاختبارات ذات فائدة ينبغي أن تكون أسرع، على الأقل في بعض الحالات، من عمليات التحقق المباشرة المذكورة في الفصل الأول. توجد نتيجة شهيرة يُطلق عليها «نظرية ويلسون»، ويتضمن تعبيرها الجبري استخدام أعداد تسمى «مضروب»، التي سنقابلها مرة أخرى في الفصل الخامس. فالعدد $n!$، الذي يُقرأ مضروب $n$، هو ناتج ضرب كل الأعداد حتى $n$. على سبيل المثال، $5! = 5 \times 4 \times 3 \times 2 = 120$. وبذلك فإن نظرية ويلسون تتجسد في عبارة بالغة الإيجاز: العدد $p$ هو عدد أولي فقط إذا كان $p$ عاملًا من عوامل $(p-1)! + 1$.

بَرْهنة هذه النتيجة ليست صعبة للغاية، وفي الواقع تتَّسم بأنها شبه بديهية في أحد الجوانب: إذا كان $p$ عددًا مركبًا — بحيث إن $p = ab$ مثلًا — وبما أن $a$ و$b$ أقل من $p$،

فإنهما عاملان من عوامل $(p-1)!$؛ ومن ثم فإن $p$ يقبل القسمة على هذا المضروب أيضًا. ويتبع ذلك أنه عند قسمة $(p-1)!+1$ على $p$، سوف يتبقى لدينا 1. (الحالة التي يتساوى فيها $a$ و$b$ تتطلب تفكيرًا أكثر قليلًا.) وهذا يذكِّرنا بمبرهنة إقليدس لعدم تناهي الأعداد الأولية. ويستتبع ذلك أنه إذا كان $p$ من عوامل $(p-1)!+1$ فإنه لا بد أن يكون $p$ عددًا أوليًّا. والعكس أصعب قليلًا في الإثبات: إذا كان $p$ عددًا أوليًّا، فإن $p$ عامل من عوامل $(p-1)!+1$. مع ذلك، فهذا هو الاتجاه المفاجئ للنظرية، مع أنه يمكن للقارئ بسهولةٍ التحققُ من صحة حالات معينة: على سبيل المثال، العدد الأولي 5 بالفعل عامل من عوامل $25 = 24+1 = 4!+1$.

إن ما تفعله نظرية ويلسون هو تحويل مسألة تحديد ما إذا كان $p$ عددًا أوليًّا أم لا، من سلسلة من مسائل القسمة (التحقق من القسمة على كل الأعداد الأولية حتى $\sqrt{p}$) إلى مسألة قسمة واحدة. مع ذلك، فالمقسوم عليه في مسألة القسمة — $(p-1)!+1$ — ضخمٌ حتى بالنسبة للقيم الصغيرة إلى حدٍّ بعيد للعدد $p$. وعلى الرغم من تجسيدها في عبارة مقتضبة، فليس لنظرية ويلسون فائدة حقيقية في تحديد أعداد أولية معينة. على سبيل المثال، إن التحقق مما إذا كان العدد 13 عددًا أوليًّا أم لا باستخدام نظرية ويلسون يتطلب منا التحقق مما إذا كان العدد 13 عاملًا من عوامل $12!+1 = 479,001,601$. (ولكن بتطبيق اختبار قابلية القسمة المذكور في الفصل الأول على العدد 13، يمكن للقارئ أن يتحقق من صحة نظرية ويلسون!) قارِنْ هذه الطريقة بالعمل اللازم للتحقق ببساطة من أن 13 غير قابل للقسمة على 2 و3. ومع أن نظرية ويلسون ليست مفيدة في التحقق من الأعداد الأولية، فإنها تمتلك ما هو أكبر من القيمة الشكلية، ويمكن استخدامها في إثبات النتائج النظرية الأخرى.

وكملاحظة أخيرة، يمكننا استغلال أعداد المضروب، التي لها الكثير من العوامل على نحو مقصود، من أجل إثبات أنه لا يمكن لمتتالية حسابية من الأعداد؛ أيْ متتالية بالصورة $a, a+b, a+2b, a+3b, \ldots$، أن تتكون من أعداد أولية «فقط»؛ إذ إنه من الممكن إيضاح أن الفجوة بين الأعداد الأولية المتعاقبة يمكن أن تكون كبيرة على نحو عشوائي، بينما الفارق المشترك بين العناصر المتعاقبة للمتتالية السابقة ثابت عند $b$. لإدراك ذلك، انظر إلى متتالية الأعداد الصحيحة المتعاقبة للعدد $n$:

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots, (n+1)!+n+1.$$

كل عدد من هذه الأعداد مركب؛ حيث إن الأول يقبل القسمة على 2 (لأن الطرفين كلاهما يتضمن 2 كعامل)، والثاني يقبل القسمة على 3، والثالث يقبل القسمة على 4، وهكذا حتى آخر عدد في القائمة، يكون $n + 1$ من عوامله. ومن ثم، فإن لدينا لأي عدد $n$ متتالية أعداد متعاقبة ليس أيٌّ منها عددًا أوليًّا.

بدلًا من التركيز على الأعداد ذات العوامل القليلة (الأعداد الأولية)، سوف نتحول في الفصل التالي إلى الأعداد ذات العوامل الكثيرة، مع أننا سنكتشف هنا أيضًا وجود روابط مدهشة لبعض الأعداد الأولية الخاصة للغاية.

الفصل الثالث

# الأعداد الكاملة والأعداد غير الكاملة

## الأعداد الكاملة

من السهل غالبًا اكتشاف الخصائص الغريبة التي تُميِّز الأعداد الصغيرة؛ على سبيل المثال، 3 هو العدد الوحيد الذي يساوي مجموع كل الأعداد السابقة له، بينما 2 هو العدد الأولي الزوجي الوحيد (مما يجعله أغرب الأعداد الأولية على الإطلاق). وللعدد 6 مزيَّة فريدة للغاية؛ هي أنه مجموع وحاصل ضرب كل عوامله الأصغر منه: $3\times2\times1 = 3+2+1 = 6$.

أطلق الفيثاغورسيون على الأعداد التي على غرار 6 «أعدادًا كاملة»؛ بمعنى أن العدد يساوي مجموع عوامله الحقيقية، كما نطلق عليها. وهي الأعداد التي يقبل العدد القسمة عليها وتكون أصغر منه. هذا النوع من الكمال نادر للغاية بالفعل. وأول خمسة أعداد كاملة هي 6 و28 و496 و8128 و33,550,336. توجد الكثير من المعلومات المعروفة عن الأعداد الزوجية الكاملة، ولكن حتى يومنا هذا لم يستطع أحد الإجابة عن سؤال القدماء ما إذا كان يوجد عددٌ لا متناهٍ من هذه الأعداد المميزة. أكثر من ذلك أنه لم يجد أحد عددًا فرديًّا من هذه الأعداد، ولم يُثبت أحد عدم وجودها. لا بد لأي عدد فردي كامل أن يكون كبيرًا على نحو ضخم، وتوجد قائمة طويلة بالسمات التي يجب على مثل هذا العدد امتلاكها نتيجة لكماله الفريد. مع ذلك، لم تتسبب كل هذه القيود في عدم ظهور مثل هذا العدد حتى الآن؛ من الجائز أن تكون وظيفة هذه السمات الخاصة هي توجيه بحثنا نحو أول عدد فردي كامل بعيد المنال، الذي ربما لا يزال منتظرًا أن يكتشفه أحد.

كان إقليدس يعلم أن الأعداد الزوجية الكاملة ترتبط ارتباطًا وثيقًا بمتتاليةٍ من الأعداد الأولية خاصةٍ للغاية وتُعرف لدينا باسم «أعداد ميرسين الأولية»؛ التي سمِّيَت على اسم مارين ميرسين (١٥٨٨–١٦٤٨)، وهو راهب فرنسي عاش في القرن السابع عشر.

يتكون عدد ميرسين $m$ من المعادلة $2^p - 1$؛ حيث $p$ عدد أولي. وإذا كانت — على سبيل المثال — أول أربعة أعداد أولية هي: 2 و3 و5 و7، فإن أول أربعة من أعداد ميرسين هي: 3 و7 و31 و127، ويمكن أن يدرك القارئ بسرعةٍ أنها أعداد أولية. إذا لم يكن $p$ عددًا أوليًّا، بافتراض أن $p = ab$ مثلًا، فإن $m = 2^p - 1$ ليس عددًا أوليًّا أيضًا بالتأكيد؛ إذ إنه يمكن تأكيد صحة أن $2^a - 1$ في هذه الظروف من عوامل العدد $m$. مع ذلك، إذا كان $p$ عددًا أوليًّا، فإن عدد ميرسين الموازي غالبًا ما يكون عددًا أوليًّا، أو هكذا يبدو.

أوضح إقليدس عام ٣٠٠ قبل الميلاد أنه عندما يوجد لديك عدد ميرسين أولي، فإنه يوجد عدد كامل يتواجد معه، وهذا العدد هو $P = 2^{p-1}(2^p - 1)$. ويمكن للقارئ أن يتحقق سريعًا بالفعل من صحة أن أول أربعة أعداد ميرسين أولية تعطي أول أربعة أعداد كاملة مذكورة آنفًا: على سبيل المثال، باستخدام العدد الأولي الثالث 5 كنقطة انطلاق نحصل على العدد الكامل $P = 2^4(2^5 - 1) = 16 \times 31 = 496$، وهو العدد الكامل الثالث في القائمة السابقة. (عوامل العدد $P$ هي قوى العدد 2 حتى $2^{p-1}$، مع قائمة الأرقام نفسها المضروبة في العدد الأولي $2^p - 1$. إنها الآن تمرينٌ على جمعِ ما يطلق عليه «متسلسلة هندسية» (ستُشرح في الفصل الخامس) للتحقق من أن العوامل الحقيقية للعدد $P$ تصل بالفعل عند جمعها إلى قيمة $P$.)

علاوة على ذلك، في القرن الثامن عشر أثبت عالم الرياضيات السويسري الكبير ليونهارت أويلر (١٧٠٧–١٧٨٣) معكوسَ الصيغة السابقة بأن كل عدد زوجي كامل هو من هذا النوع. وبهذه الطريقة حقَّقَ إقليدس وأويلر مطابقة بين كل عدد من أعداد ميرسين الأولية وكل عدد من الأعداد الزوجية الكاملة. مع ذلك، فالسؤال الطبيعي التالي هو: هل كل أعداد ميرسين أولية؟ للأسف لا، وإثبات هذا الأمر قريب للغاية؛ إذ إن عدد ميرسين الخامس يساوي $2^{11} - 1 = 2,047 = 23 \times 89$. في الواقع نحن لا نعرف حتى ما إذا كانت متتالية أعداد ميرسين الأولية ستنتهي أم لا؛ ربما بعد نقطة معينة سوف تصبح كل أعداد ميرسين أعدادًا مركبة.

مع ذلك، فأعداد ميرسين مرشحة بالمثل لأنْ تكون أعدادًا أولية طبيعية؛ إذ إنه يمكن إثبات أن أي قاسم (عامل) حقيقي — إذا وُجد — من قواسم عدد ميرسين $m$ يمتلك المعادلة المميزة للغاية $2kp + 1$. على سبيل المثال، عندما يكون $p = 11$، ومن خلال هذه النتيجة نحتاج فقط أن نتحقق من قابلية القسمة على الأعداد الأولية ذات

الصيغة $22k + 1$. ويتطابق العاملان الأوليان 23 و89 مع قيمة $k = 1$ وقيمة $k = 4$ على التوالي. تمدنا هذه الحقيقة حول قواسم أعداد ميرسين أيضًا بشيء إضافي؛ إذ إنها تقدم لنا طريقة ثانية لرؤية أنه لا بد من وجود عدد لا متناهٍ من الأعداد الأولية؛ حيث إنها تبيِّن أن أصغر قاسم أولي للمعادلة $2^p - 1$ يتخطى $p$؛ ومن ثم فإن $p$ لا يمكن أن يكون أكبر عدد أولي. ولما كان هذا ينطبق على كل عدد أولي $p$، نستنتج أنه لا يوجد أكبر عدد أولي، وأن متتالية الأعداد الأولية تستمر للأبد.

نظرًا لأننا لا نمتلك طريقة لإنتاج الأعداد الأولية بإرادتنا، فإنه يوجد — دائمًا — أكبر عدد أولي معروف، وفي الوقت الراهن، أكبر عدد أولي دائمًا ما يكون عدد ميرسين الأوليَّ، وذلك بفضل المشروع الدولي «البحث الكبير عن أعداد ميرسين الأولية في الإنترنت» (جي آي إم بي إس)، وهو مشروع تعاوُنيٌّ بين مجموعة من المتطوعين بدأ في عام ١٩٩٦. يستخدم المشروع آلاف أجهزة الكمبيوتر الشخصية التي تعمل على نحو متوازٍ على اختبار أولية أعداد ميرسين باستخدام مزيج من الخوارزميات المصممة خصوصًا لهذا الغرض. والعدد الأكبر حاليًّا في العالم الذي أُعلن في أغسطس ٢٠٠٨ هو $2^p - 1$؛ حيث $p = 43,112,609$، على الرغم من اكتشاف عدد ميرسين جديد في أبريل ٢٠٠٩؛ حيث $p = 42,643,801$. ويتكون هذان العددان من حوالي ثلاثة عشر مليون خانة وسيتطلبان آلاف الصفحات من أجل كتابتهما بنظام العد العشري العادي.

## الأعداد غير الكاملة

ترتكز المعرفة العادية للأعداد التقليدية على الأعداد المنفردة التي يُعتقد أنها تمتلك خصائص مميزة — إن لم تكن سحرية — على غرار الأعداد الكاملة. مع ذلك، فإن من أزواج الأعداد التي لها سمات مماثلة 220 و284، وهما أول «زوج عددي متحابٍّ»؛ بمعنى أن مجموع العوامل الحقيقية لكل عدد منهما يساوي العدد الآخر؛ وهو نوع من الكمال الذي يشمل زوجًا من الأعداد. اكتَشف عالمُ الرياضيات الفرنسي الهاوي الشهير بيير دي فيرما (١٦٠١–١٦٦٥) أزواجًا أخرى من الأعداد المتحابة مثل العدد 17، 296 والعدد 18، 416، في حين اكتشف أويلر عشرات الأزواج الأخرى. والمثير للعجب أن كليهما أغفل الزوج الصغير 1184 و1210، الذي اكتشفه نيكولو باجانيني في عام ١٨٦٦ عندما كان في السادسة عشرة من عمره. ويمكننا بالطبع محاولة تخطي الأزواج والبحث عن الثلاثيات والرباعيات، وما إلى ذلك. فالدورات الأطول نادرة ولكنها تظهر على نحو بارز.

يمكننا أن نبدأ بأي عدد، ونجد مجموع قواسمه الصحيحة، ونكرر العملية حيث نكوِّن ما يطلق عليه «متتالية القواسم الكاملة» للعدد. غالبًا ما تكون النتيجة محبطة قليلًا؛ إذ نحصل نموذجيًّا على سلسلة تتوجه نحو 1 على نحو سريع جدًّا، وهي النقطة التي تتوقف عندها العملية. على سبيل المثال، حتى عند البدء بعدد يبدو واعدًا على غرار 12، فإن السلسلة تكون قصيرة:

$$12 \longrightarrow (1+2+3+4+6)$$

$$= 16 \longrightarrow (1+2+4+8)$$

$$= 15 \longrightarrow (1+3+5) = 9$$

$$9 \longrightarrow (1+3) = 4 \longrightarrow (1+2) = 3 \longrightarrow 1.$$

المشكلة هي أنك بمجرد أن تصل لعدد أولي، فقد انتهى الأمر. والأعداد الكاملة بالطبع استثناءات، فكلٌّ منها يقدم لنا دورة واحدة صغيرة، بينما تؤدي الأزواج المتحابَّة إلى دورتين:

$$220 \longrightarrow 284 \longrightarrow 220 \longrightarrow \cdots$$

ويُطلق على الأعداد التي تؤدي إلى أكثر من دورتين «أعداد اجتماعية». ولم تُدرس مطلقًا حتى القرن العشرين؛ إذ لم يَكتشف أحدٌ أيًّا منها. وحتى الآن لم يُكتشف عدد يؤدي إلى دورات ثلاثية، مع أنه يوجد في الوقت الحالي 120 دورة رباعية معروفة. واكتشف بي بوليه في عام ١٩١٨ أول الأمثلة على ذلك. والدورة الأولى خماسية، وهي:

$$12,496 \longrightarrow 14,288 \longrightarrow 15,472 \longrightarrow 14,536 \longrightarrow 14,264 \longrightarrow 12,496.$$

مثال بوليه الثاني مدهش للغاية، وحتى يومنا هذا لم تُكتشف أية دورة أخرى تكاد تضاهيها؛ إذ تبدأ بالعدد 14,316 ونحصل منه على دورة من ثمانية وعشرين عددًا. وكل الدورات الأخرى المعروفة لا يتخطى طولُها عشرةَ أعداد. ولا توجد أيةُ نظريات حتى الوقت الراهن حول الأعداد المتحابة والأعداد الاجتماعية تضاهي جمال نظريتَي إقليدس وأويلر للأعداد الكاملة. مع ذلك، قادت طاقة الحوسبة الحديثة إلى شيء من النهضة التجريبية في هذا المجال، ويوجد المزيد مما يمكن قوله عن ذلك.

يمكننا تقسيم كل الأعداد إلى ثلاثة أنواع: «أعداد ناقصة» و«أعداد كاملة» و«أعداد زائدة»، وفقًا لكَوْنِ مجموع قواسمها الحقيقية أقلَّ من العدد نفسه أو مساويًا له أو أكبر منه. على سبيل المثال، وكما رأينا بالفعل، فإن العدد 12 عدد زائد، وكذلك 18 و24؛ إذ إن مجموع قواسمهما الحقيقية على التوالي هو 21 و36.

إن البحث البسيط عن الأعداد الصحيحة الزائدة قد يقودك إلى تخمين أنها ببساطةٍ مضاعفاتُ العدد 6. بالتأكيد أيُّ عدد أكبر من 6 في صورة $6n$ هو عدد زائد؛ حيث إن عوامل $6n$ يجب أن تتضمن 1 و2 و3 معًا مع $n$ و$2n$ و$3n$، يكون مجموعها أكبر من العدد الأصلي $6n$. مع ذلك، يمكن توسيع نطاق هذه الملاحظة لنبين أن الأعداد الزائدة لا تقتصر فقط على مضاعفات 6؛ إذ يمكن أن نقول الأمر نفسه على أي عدد كامل $k$. فعوامل $nk$ سوف تتضمن 1 مع كل عوامل العدد الكامل $k$، كلٌّ منها مضروب في $n$؛ وبهذا سيزيد مجموع كل العوامل الحقيقية للعدد $nk$ على الأقل إلى $nk + 1$؛ ومن ثم فإن أي مضاعف لعدد كامل سوف يكون عددًا زائدًا. على سبيل المثال، 28 عدد كامل؛ ومن ثم فإن $56 = 28 \times 2$ و$84 = 28 \times 3$، وما إلى ذلك، جميعها أعداد زائدة.

ومن هذا ندرك أن مضاعفات الأعداد الكاملة ومضاعفات الأعداد الزائدة — على نفس المنوال — أعدادٌ زائدة. وبالتوصل لهذا الاكتشاف، ربما لا تزال تخمن أن كل الأعداد الزائدة هي ببساطة مضاعفات للأعداد الكاملة. مع ذلك، فليس عليك البحث طويلًا من أجل اكتشاف أول استثناء لهذا التخمين؛ إذ إن 70 عدد زائد، ولكن لا يوجد بين عوامله عدد كامل. وبالفعل العدد 70 هو أول عدد يطلق عليه أنه غريب، ولكن ليس لهذا السبب بالضبط (ومصدر هذه التسمية مذكور لاحقًا).

على الرغم من هذه الاكتشافات، ربما تظل معتقدًا على الأرجح أنه على غرار عدم وجود أعداد كاملة فردية، لا يوجد أعداد زائدة فردية أيضًا. بعبارة أخرى، ربما يكون تخمينُنا المعدل هو أن كل الأعداد الفردية ناقصة. يبدو أن حساب مجموع القواسم الصحيحة لبضع مئات قليلة من الأعداد الفردية الأولى يؤكد هذه النظرية، ولكن يتضح خطأ هذا الادعاء في النهاية عند اختبار العدد 945، الذي يصل مجموع قواسمه الحقيقية إلى 975. والآن أصبح بالإمكان القول بأن أي مضاعف من مضاعفات الأعداد الزائدة هو عدد زائد، وتُقدم لنا المضاعفات الفردية للعدد 945 عددًا لا متناهيًا من الأعداد الزائدة الفردية.

ومع ذلك، إذا تصرفنا على نحو أكثر ذكاءً، يمكننا أن نكتشف هذا المثال الداحض بسرعةٍ أكبر من اختبارنا عددًا فرديًّا بعد آخَر دون تفكير. لكي يكون للعدد مجموع قواسم حقيقية كبير، فإنه يلزم وجود الكثير من العوامل، والعوامل الكبيرة بينها تأتي في حد ذاتها من خلال اقترانها بالعوامل الصغيرة. ومن ثم يمكِننا تكوين أعداد ذات مجموع قواسم صحيحة كبيرة عن طريق ضرب أعداد أولية صغيرة معًا. إذا كنا نركز على الأعداد الفردية فحسب، ينبغي أن نتوجه نحو الأعداد الناتجة عن الأعداد الأولية الفردية القليلة الأولى، وهي 3 و5 و7، وما إلى ذلك. وستقودك هذه القاعدة الأساسية سريعًا إلى اختبار $945 = 7 \times 5 \times 3^3$؛ ومن ثم ستكتشف خاصية الزيادة بين الأعداد الفردية أيضًا.

ليس خافيًا أن أصغر مثال لعدد يحمل سمات معينة كبيرٌ نوعًا ما. وهذا حقيقي على نحو خاص إذا كانت السمات المعنيَّة تكوِّن ضمنيًّا بنية من العوامل المعينة في الأعداد اللازمة. وحينها يمكن أن يصبح أصغر مثال عددًا عملاقًا، مع أنه ليس صعبَ الاكتشافِ بالضرورة، إذا استغللنا السمات المعطاة خلال سَعْينا للوصول للحل. أحد الأمثلة لِلُغْزٍ عددي من هذا النوع هو إيجاد أصغر عدد يساوي خمسة أضعاف عدد مكعب، وثلاثة أضعاف عدد مرفوع للقوة 5. الإجابة عن هذا اللغز هي:

$$7,119,140,125 = 5 \times 1125^3 = 3 \times 75^5.$$

مع ذلك، ليس من الصعب إدراك السبب في أن أصغر حل لهذه المسألة عدد بالمليارات. فأي حل $n$ يجب أن يتضمن الصيغة $3^r5^sm$؛ حيث تكون $r$ و$s$ قوتين موجبتين، وتُجمَع كلُّ العوامل الأولية الباقية معًا لتكوِّن العدد الصحيح $m$ الذي لا يقبل القسمة على 3 أو 5. إذا ركزنا أولًا على القيم المحتملة للعدد $r$، نلاحظ أنه نظرًا لأن $n$ خمسة أضعاف عدد مكعب، لا بد أن يكون الأس $r$ من مضاعفات 3، ونظرًا لأن $n$ ثلاثة أضعاف عدد مرفوع للقوة الخامسة، فإن العدد $r - 1$ ينبغي أن يكون من مضاعفات 5. أصغر عدد $r$ يتفق مع هذين الشرطين في الوقت نفسه هو $r = 6$. وعلى المنوال نفسه، ينبغي أن يكون الأس $s$ من مضاعفات 5، بينما ينبغي أن يكون $s - 1$ من مضاعفات 3، وأقل $s$ يتوافق مع الشروط هو $s = 10$. ولِجَعْل $n$ في أصغر صورة ممكنة، نضع $m = 1$؛ وبهذا يكون $n = 3^6 \times 5^{10} = 3(3 \times 5^2)^5 = 3 \times 75^5$؛ ومن ثم فإن $n$ يكون بالفعل ثلاثة أضعاف عدد مرفوع للقوة الخامسة، وفي الوقت نفسه $n = 5(3^2 \times 5^3)^3 = 5 \times 1125^3$، وهكذا يكون $n$ أيضًا خمسة أضعاف عدد مكعب.

يوجد مثال شهير أكثر غرابة؛ يتمثل في مسألة الماشية المنسوبة إلى أرخميدس (٢٨٧–٢١٢ قبل الميلاد)، وهو أعظم عالم رياضيات في العصور القديمة. لم تُحل هذه المسألة حتى القرن التاسع عشر، فأصغر عدد لقطيع الماشية يتوافق مع كل الشروط الموضوعة في القصيدة الأصلية المكونة من أربعة وأربعين بيتًا يُمثَّل بعدد يزيد عدد خاناته عن مائتي ألف خانة!

التحذير الذي ينبغي استقاؤه من كل هذا هو أن الأعداد لا تُظهِر تنوُّعها الكامل إلا عندما نتوجه لعالَم الأعداد الكبيرة للغاية. ولهذا السبب، فإن مجرد حقيقة أنه لا يوجد أعداد فردية كاملة تتكون من أقل من ثلاثمائة خانة لا يخوِّلنا في حد ذاته أن نقول إنها قد لا تكون موجودة. مع ذلك، فإن بعض كبار الخبراء في هذا المجال سيندهشون إذا ظهر مثل هذا العدد.

بالعودة مرة أخرى إلى السلوك العام لمتتالية القواسم الكاملة، لا يزال يوجد سؤال لا يمكن لشخص أن يجيب عنه: ما هي الاحتمالات المتاحة لمتتالية القواسم الكاملة؟ إذا وصلَت المتتالية إلى عدد أولي، فإنها ستتوقف على الفور عند 1 دائمًا، ولا يمكن القيام بذلك بطريقة أخرى. وإذا لم يحدث ذلك، فربما تكون المتتاليةُ دوريةً وتقدِّم عددًا اجتماعيًّا. مع ذلك، توجد احتمالية أخرى ذات صلة تنكشف من خلال حساب متتالية القواسم الكاملة للعدد 95:

$$95 = 5 \times 19 \longrightarrow (1 + 5 + 19) = 25 = 5 \times 5 \longrightarrow (1 + 5)$$
$$= 6 \longrightarrow 6 \longrightarrow 6 \longrightarrow \cdots$$

ما حدث هنا هو أنه على الرغم من أن 95 ليس عددًا اجتماعيًّا، فإن متتالية قواسمه الكاملة وصلت في النهاية إلى عدد اجتماعي (أو على نحو أكثر دقة، في هذه الحالة وصلتْ إلى العدد الكامل 6) ثم بدأت في دورة.

من الجائز أن تكون هناك احتمالية واحدة باقية، وهي أن متتالية القواسم الكاملة لعدد لا تصل إلى عدد أولي أو إلى عدد اجتماعي أبدًا، وفي هذه الحالة لا بد أن تكون المتتالية سلسلة لا متناهية من الأعداد المختلفة التي لا تكون أعدادًا اجتماعية ولا أولية. هل هذا ممكن؟ ما يثير الدهشة أنه لا أحد يعرف. أما الأكثر إثارة للدهشة فهو أنه توجد أعداد صغيرة لا تزال متتاليةُ قواسمِها الكاملة غيرَ معروفة (ومن ثم فإنها تظل مرشحة

لأنْ تمتلك متتالية قواسم كاملة لا متناهية). أول هذه الأعداد الغامضة هو 276، الذي تبدأ متتاليته على هذا النحو:

$$276 \longrightarrow 396 \longrightarrow 696 \longrightarrow 1104 \longrightarrow 1872 \longrightarrow 3770 \longrightarrow 3790$$

$$\longrightarrow 3050 \longrightarrow 2716 \longrightarrow 2772 \longrightarrow \cdots$$

ولكن لا يعرف أحد أين تنتهي بالضبط.

ربما يودُّ القارئ أن يستكشف هذا الأمر بنفسه قليلًا، وفي هذه الحالة ينبغي أن أُطْلعك على سرِّ كيفية حسابِ ما يطلق عليه «دالة القواسم الكاملة $a(n)$» من عملية تحليل العدد $n$ لعوامله الأولية: خذ كل نواتج ضرب الحدود $(p^{k+1} - 1)/(p - 1)$؛ حيث $p^k$ هو أعلى قوة أولية للعدد الأولي $p$ الذي يقسم $n$، ثم اطرح $n$ نفسه. على سبيل المثال: $276 = 2^2 \times 3 \times 23$؛ ومن ثم فإن:

$$a(276) = \frac{2^3 - 1}{2 - 1} \times \frac{3^2 - 1}{3 - 1} \times \frac{23^2 - 1}{23 - 1} - 276$$

$$= 7 \times 4 \times 24 - 276 = 672 - 276 = 396$$

وهو ما أُشيرَ إليه في الحد الثاني في متتالية القواسم الكاملة للعدد 276 المذكورة آنفًا.

لا يوجد نهاية لأنواع الأعداد التي يمكننا تقديمها من خلال تسمية الأعداد $n$ التي لها علاقة محددة بدالة القواسم الكاملة. وكما ذكرنا بالفعل، يكون $n$ عددًا «كاملًا» إذا كان $a(n) = n$، وعددًا «زائدًا» إذا كان $a(n) > n$. والعدد $n$ «شبه الكامل» هو العدد الذي يمثل مجموع بعض قواسمه الحقيقية (القواسم الأقل من $n$)؛ ومن ثم فإنه ينتج من هذا التعريف أن كل الأعداد شبه الكاملة إما أن تكون أعدادًا كاملة وإما أن تكون أعدادًا زائدة. على سبيل المثال، العدد 18 عدد شبه كامل؛ حيث إن $18 = 3 + 6 + 9$، ويطلق على العدد مسمًّى «غريب» إذا كان زائدًا ولكنه ليس شبه كامل، وأصغر عدد غريب هو 70.

يمكن للمرء أن يرى أن الموضوع أصبح متشعبًا للغاية في طبيعته؛ ومنْح أسماء لمجموعات محددة على نحو اعتباطي من الأعداد، في حد ذاته، لا يجعلها مثيرة للاهتمام. ينبغي أن نعرف متى نتوقف. وبالوصول إلى هذه المرحلة، من المهم إدراك أن الاستراتيجيات الأساسية المستخدمة في معالجة هذه الموضوعات الجديدة تُذكِّرُنا بما

أوضحه إقليدس وأويلر فيما يخص الأعداد الكاملة. ولسوف تتذكر أن ما أَثبتَه إقليدس هو أنه إذا كان عدد ميرسين عددًا أوليًّا، فإن عددًا آخر كان زوجيًّا وكاملًا. بعد ذلك أَثبتَ أويلر على نحو معاكس أن كل الأعداد الزوجية الكاملة تَظهر بهذه الطريقة. وفي القرن التاسع أَثبتَ عالِم الرياضيات الفارسي ثابت بن قرة أنه لأيِّ عدد $n$ ثلاثةُ أعداد — إذا كانت كلها أولية — تسمح بتكوين زوج من الأعداد المتحابة. وعَمَّمَ أويلر نظريةَ ثابتٍ بعد ذلك في القرن الثامن عشر، ولكن حتى هذه المعادلة المحسنة يبدو أنها لا تُنتج إلا أزواجًا متحابة قليلة، وأنه يوجد أزواج متحابة كثيرة لا تَنتج عن تكوين هذا الزوج. (يُعرَف الآن ما يقرب من اثني عشر مليون زوج من الأزواج المتحابة.) وفي العصور الحديثة، وضع كرافيتز طريقة مشابهة لتكوين أعداد غريبة من أعداد معينة ينبغي أن تكون أولية، ووَجدت هذه الصيغةُ بنجاح عددًا غريبًا ضخمًا للغاية يتكون من أكثر من خمسين خانة.

لقد أسهم هذان الفصلان في تعريف القارئ بالعوامل وعملية تحليل الأعداد الطبيعية — أو «الأعداد الصحيحة الموجبة» كما تُعرف أيضًا — إلى عوامل، وتوضيحها باستخدام مجموعة متنوعة من الأمثلة. وهذا سيُعدُّك جيدًا للفصل التالي، والذي ستتعرف فيه على طريقة تطبيق هذه الأفكار على التشفير المعاصر؛ علم الأسرار.

الفصل الرابع

# التشفير: الحياة السرية للأعداد الأوَّلية

في هذا الفصل سوف يدرك القارئ أن مجموعة أعداد العدِّ عُرفتْ منذ العصور القديمة بأنها مخزن للألغاز والأسرار، والكثير منها لم يُحلَّ حتى الآن. هذا كافٍ بالنسبة لكثيرٍ منا من أجل تبرير الدراسة الجادة المستمرة للأعداد، ولكن ربما يكون للآخرين رأي مختلف. ولما كانت هذه الألغاز مثيرة للاهتمام وصعبة الحل، فربما يُعتقد أن لها صلة ضعيفة ببقية المعارف البشرية، ولكنَّ ذلك اعتقاد خاطئ.

تَبيَّن على مدى العقود القليلة الماضية أن الأسرار العادية؛ الأسرار التي ننغمس جميعًا فيها من وقت لآخر، يمكن أن تكون مشفَّرة في صورة عددية. هذا هو ما يحدث الآن بالفعل، ويمكن أن تكون أثمنُ أسرارنا — سواء كانت تجارية أو عسكرية، شخصية أو مالية، سياسية أو شائنة بكل ما في الكلمة من معنى — محميةً على شبكة الإنترنت عن طريق إخفائها في صورة أعداد العد العادية.

## تحوُّل الأسرار إلى أعداد

كيف يكون كل هذا ممكنًا؟ يمكن أن يُعبَّر عن أي معلومات بالكلمات، سواء كانت قصيدة أو كشف حساب مصرفي أو مخطط تصميم لسلاح أو برنامج كمبيوتر. مع ذلك، ربما نحتاج لزيادة حروفنا الأبجدية المستخدمة في تكوين كلماتنا لِما هو أكثر من الحروف الأبجدية العادية. ربما نزيد رموزًا رقمية وعلامات ترقيم، بما في ذلك رموز خاصة للمسافة بين الكلمات العادية، مع ذلك، هذه هي الحالة التي يمكن فيها التعبير عن كل المعلومات التي نرغب في نقلها — بما في ذلك تعليمات إنتاج الصور والرسوم البيانية — باستخدام كلمات من أبجدية لا تزيد، على سبيل المثال، عن ألف رمز. يمْكننا

عد هذه الرموز؛ ومن ثم نمثِّل كل رمز بعدد على نحو فريد. ونظرًا لأن الأعداد لا تكلِّف شيئًا ولا تنضب، ربما يكون من الملائم استخدامُ الأعداد كلها بعدد الخانات نفسه لهذا الغرض (لذا على سبيل المثال، يُمثل كل رمز على نحو فريد باستخدام رقم التعريف الشخصي PIN الخاص به والمكون من أربعة خانات). ويمكننا أن ننظم الرموز معًا في سلسلة بالصورة اللازمة لإنتاج عدد طويل ضخم يقدم المعلومات كلها. ويمكننا حتى العمل بالنظام الثنائي إذا أردنا؛ ومن ثم نبتكر طريقة لترجمة أية معلومات إلى سلسلة طويلة مكونة من الأصفار والآحاد. ويمكن حينها تشفير كل رسالة قد نرغب في إرسالها في صورة سلسلة ثنائية، ثم يُفك تشفيرها في الطرف الآخر عن طريق كمبيوتر مبرمج على نحو مناسب، لكي تُجمَع وتُترجَم بلغة عادية يمكننا جميعًا فهمها. هذا هو أول ما يجب إدراكه. من أجل إرسال رسالة بين شخص وآخر، يكفي — نظريًّا وعمليًّا — أن تتوافر القدرة على إرسال أعداد من شخص إلى شخص آخر.

ومع ذلك، فإن تحويل الرسائل إلى أعداد ليس في حد ذاته الفكرةَ المذهلة؛ إذ من المؤكد أن العملية نفسها التي تُحوَّل فيها كلُّ المعلومات إلى صيغة عددية ربما تكون مَخْفِيَّة عن العامة، ولكنها مع ذلك ليست مصدر الحماية ضد المتلصصين. في الواقع، من وجهة نظر علم التشفير، ربما نحدد أي رسالة — أو «نص عادي» كما يُطلق عليها — من خلال العدد الذي يمثلها؛ ومن ثم ننظر للعدد على أنه النص العادي نفسه؛ حيث من المفترض أن يستطيع أي شخصٍ الوصولَ للوسيلة التي ستسمح بتحول إحدى صور النص إلى صورة أخرى. ولا تُعتبر السرِّيةُ بالفعل سرِّيةً إلا عندما نُخفي أعداد النص العادي باستخدام أعداد أخرى.

اسمح لي أن أعرفك على الرموز الزائفة الموجودة في السيناريوهات المختلفة للتشفير، التي تعبر عن دراسة الشفرات (الأكواد السرية). سنتخيل أن أليس وبوب يرغبان في التواصل معًا دون أن تَسْتَرِقَ إيف — المتنصتة — السمع إليهما. ربما نتعاطف مع أليس وبوب على نحو غريزي ونرى أفعال إيف سيئة، ولكن بالطبع قد يكون العكس هو الصحيح؛ إذ قد تمثل إيف سلطة شُرطِيَّة شريفة تكافح من أجل حمايتنا من مؤامرات بوب وأَلِيس الشريرة.

أيًّا كانت المواقف الأخلاقية للأشخاص الثلاثة، توجد طريقة عتيقة يمكن أن يستخدمها بوب وأليس من أجل إخراج إيف خارج المحادثة بينهما، حتى لو اعترضت إيف الرسائلَ المتبادلة بينهما؛ فيمكنهما تشفير البيانات باستخدام مفتاح تشفير لا

يعرفه إلا أليس وبوب. ما يمكنهما فعله هو التقابل في بيئة آمنة يتبادلان فيها عددًا سريًّا (57 مثلًا) ثم يعودان كلٌّ إلى منزله. وعندما يحين الوقت، سترغب أليس في إرسال رسالة إلى بوب، ولنفترضْ أن الرسالة يمكن تمثيلها — لمجرد توضيح الفكرة — بعدد من خانة واحدة بين 1 و9. وفي اليوم الموعود، ترغب أليس في إرسال رسالة 8 إلى بوب. فتأخذ الرسالة وتضيف إليها المكون السري؛ أيْ تخفي قيمتها الحقيقية بإضافة 57 ثم ترسل الرسالة $65 = 57 + 8$ إلى بوب عن طريق قناة تواصل غير آمنة. فيتسلم بوب هذه الرسالة ويطرح منها العدد السري للحصول على النص العادي لرسالة أليس $65 - 57 = 8$.

مع ذلك، تدرك إيف الشريرة ما ينوي هذان الاثنان فعله، وبالفعل تنجح في اعتراض الرسالة المشفرة 65. ولكن ماذا يمكن أن تفعل بها؟ ربما تعلم — كما نعلم نحن أيضًا — أن أليس أرسلت رسالة من بين تسع رسائل محتملة 1، 2، 3، ...، 9 إلى بوب، وتعلم أيضًا أنها شفَّرَتها بإضافة عدد للرسالة، لا بد أنه يقع بين $56 = 9 - 65$، و$64 = 1 - 65$. مع ذلك، نظرًا لأنها لا تستطيع معرفة أيٍّ من هذه الأعداد المخفية تم استخدامه (فهي ليست على علم بالسر)، فإنها لا تعلم النص العادي الفعلي للرسالة التي أرسلَتْها أليس إلى بوب، الذي لا يزال على الأرجح أحد الاحتمالات التسعة. وكل ما تعرفه هو أن أليس أرسلت رسالة إلى بوب، ولكنها لا تعرف محتواها.

قد يبدو أنَّ أليس وبوب محصَّنان الآن من شر إيف ويمكنهما التراسل على نحو آمن باستخدام العدد السحري 57 من أجل إخفاء كل ما يريدان قوله. لكن الأمر ليس كذلك. فالأجدر بهما تغيير ذلك العدد، بل الأفضل استخدام عدد سري جديد كل مرة؛ لأنهما إن لم يفعلا ذلك فسوف يبدأ النظام في تسريب معلومات لإيف. على سبيل المثال، لِنَقُلْ إنه بعد أسبوع ترغب أليس في إرسال نفس رسالة العدد 8 إلى بوب. فحينها، سيسير كل شيء كما حدث من قبل، وسوف تعترض إيف مرة أخرى العدد الغامض 65 من موجات البث، ولكن هذه المرة سوف يخبرها شيئًا. سوف تعلم إيف أنه أيًّا كانت الرسالة، فهي الرسالة نفسها التي أرسلتها أليس إلى بوب في الأسبوع الأول؛ وهذا شيء لا يرغب أليس وبوب في أن تعرفه إيف.

غير أن ذلك لا يمثل مشكلة كبيرة لأليس وبوب. فعندما تقابلا في المرة الأولى لتبادُل مفتاح الشفرة، كان يمكن لأليس أن تقدم لبوب قائمة طويلة مرتبة من آلاف الأعداد السرية — بدلًا من الاتفاق على عدد واحد سريٍّ فحسب — حيث يُستخدم واحد تلو

الآخر؛ ومن ثم يتجنبان أية احتمالية لوقوع مصادفات ذات معنًى في عمليات التواصل المتاحة على نحو علني.

وهذا بالفعل ما يحدث في الواقع. ويُطلق على هذا النوع من نظم التشفير «دفتر المرة الواحدة»؛ إذ يُخفي المرسل والمتلقي النص العادي بعدد من الدفتر يُستخدم لمرة واحدة، ثم يتخلى المرسل والمتلقي عن هذه الورقة (العدد) من الدفتر بعد إرسال الرسالة وفك تشفيرها. وتمثِّل طريقة دفتر المرة الواحدة نظامًا آمنًا تمامًا؛ إذ إن الرسائل غير المؤمَّنة التي تنتقل في العلن لا تحتوي على أية معلومات حول محتوى النص العادي. ولفك تشفيرها يحتاج الشخص المعترِض للرسالة إلى الحصول على هذا الدفتر من أجل التوصُّل إلى مفتاح التشفير وفك التشفير.

## المفاتيح وتبادل المفاتيح

يبدو أن مشكلة التواصل الآمن حُلتْ بالكامل بواسطة دفتر المرة الواحدة، وهذا حقيقي نوعًا ما. مع ذلك، تتمثل مشكلة الشفرات التي على شاكلة دفتر المرة الواحدة في أنها تتطلب من الطرفين تبادُل المفتاح من أجل استخدامها. ويتطلب ذلك في الواقع الكثيرَ من الجهد. وبالنسبة للاتصالات عالية المستوى — على غرار الاتصالات بين البيت الأبيض والكرملين — لا يمثِّل المالُ مشكلة، ويَحْدث التبادل اللازم تحت ظروف أَمنيَّة عالية المستوى. على الجانب الآخر، يحتاج الأشخاص والمؤسسات كافةً في المعاملات اليومية للتواصل بعضُهم مع بعض على نحو سري. ولا يستطيع الطرفان تحمُّل الوقت والطاقة اللازمَين لتأمين تبادُل المفتاح، وحتى إذا تم تأمين هذا عن طريق طرف ثالث موثوق فيه، يمكن أن تكون العملية مكلِّفة للغاية.

إن موطن الضعف في كل الشفرات التي استُخدمت لآلاف السنوات حتى سبعينيات القرن العشرين هو أنها كانت «شفرات متماثلة» كلها؛ مما يعني أن التشفير وفك التشفير كانا يَتِمَّان باستخدام مفتاح واحد. وسواء كانت الشفرات بسيطة، عبارة عن تغيير في ترتيب الحروف الأبجدية البسيطة كالتي استخدمها يوليوس قيصر، أو معقدة كشفرة إنيجما المعقدة التي استخدمت في الحرب العالمية الثانية، فقد عانت جميعها من موطنِ ضعفٍ مشترك؛ هو أنه بمجرد أن يعرِف العدو كيفية تشفيرك لرسائلك، يمكنه فك تشفيرها تمامًا كما تفعل أنت. ومن أجل الاستفادة من الشفرة المتماثلة يحتاج الطرفان المتواصلان تبادُل مفتاح الشفرة على نحو آمن.

يبدو أنه افتُرِض ضمنًا أن هذا مبدأ لا مفرَّ منه في الشفرات السرية؛ فمن أجل استخدام الشفرة يحتاج الطرفان، بطريقة أو بأخرى، تبادُلَ مفتاح الشفرة وإبقاءه سرًّا عن الأعداء. وبالطبع ربما يعبِّر هذا الأمر عن منطق رياضي سليم.

وهذا نوع من الافتراض يثير الشك لدى علماء الرياضيات. فنحن نتعامل مع موقف رياضي في الأساس؛ لذا قد يتوقع المرء ترسيخ هذا المبدأ على أسس قوية وتمثيله من خلال نظرية رياضية. بَيْدَ أنه لا توجد مثل هذه النظرية، والسبب في عدم وجود مثل هذه النظرية هو أن هذا المبدأ ببساطة ليس صحيحًا، كما تكشف التجربة الفكرية التالية.

لا يتطلب النقل الآمن لرسالةٍ من أليس لبوب — في حد ذاته — تبادُل مفتاح الشفرة؛ حيث يمكنهما متابعة الأمر كما يلي. تكتب أليس النص العادي لرسالتها لبوب، وتضعه في صندوق تؤمنه من خلال قفل، على أن تملك هي فقط مفتاح هذا القفل، ثم ترسل الصندوق إلى بوب الذي لا يستطيع بالطبع فتْحه، غير أن بوب يضيف قفلًا آخر للصندوق، الذي يمتلك هو وحده مفتاحه، وبعد ذلك يُعاد الصندوق إلى أليس، فتزيل قفلها عنه، وترسله للمرة الثانية إلى بوب، وهذه المرة يفتح بوب الصندوق ويقرأ رسالة أليس على نحو آمن؛ إذ لديه عِلم بأن إيف المتطفلة لم تستطع اختلاس النظر لمحتويات الصندوق خلال عملية التسليم. وبهذه الطريقة يمكن إرسال رسالة سرية إرسالًا آمنًا — باستخدام قناة تواصل غير آمنة — دون أن يتبادل أليس وبوب المفاتيح. يبين هذا السيناريو الخيالي أنه لا يوجد قانون ينص على وجوب تبادل المفتاح خلال تبادل الرسائل المؤمَّنة. وفي النظام الحقيقي، ربما يكون مفتاح أليس وبوب هو شفرتهما الخاصة للرسالة وليس شيئًا ماديًّا يمنع المتلصصين المحتملين من الوصول للنص العادي. وربما يستخدم أليس وبوب هذا التبادل الأول فيما بعدُ لإرساء شفرة متماثلة عادية يمكن أن تُستخدم في إخفاء كل الاتصالات المستقبلية.

في الحقيقة، هذه هي الطريقة التي غالبًا ما تنشأ من خلالها قناة تواصل غير آمنة في العالم الواقعي. مع ذلك، فاستبدال الشفرات الشخصية بالأقفال المادية ليس أمرًا سهلًا. فعلى النقيض من الأقفال، يمكن أن تتداخل شفرتا أليس وبوب معًا؛ مما يجعل فك التشفير (أي فتح القفل) الذي تقوم به أليس أولًا ثم بوب لا ينجح. مع ذلك، كان وايتفيلد ديفي ومارتن هيلمان أول من أثبت علنًا أن هذه الطريقة يمكن أن تكون فعالة في عام ١٩٧٦.

يوجد منهج آخر ذو صلة هو «التشفير غير المتماثل» أو «التشفير بالمفتاح العام»، وفيه يعلِن كلٌّ شخص عن مفتاحه العام الذي يستخدم لتشفير الرسائل المرسلة للشخص

الآخر. بيد أن كل شخص يحمل أيضًا مفتاحًا خاصًّا لا يمكن بدونه قراءة الرسائل المشفرة باستخدام مفتاحه العام الفريد. وباستخدام تشبيه القفل، تُقَدِّم أليس لبوب صندوقًا يضع فيه النص العادي لرسالته مع قفل مفتوح (مفتاحها العام) تمتلك هي فقط مفتاحه (مفتاحها الخاص).

قد يبدو نظام المفتاح العام العملي مَطلبًا مبالغًا فيه؛ إذ إن المطلبين المتلازمين — الأمان وسهولة الاستخدام — يبدوان متعارضين. غير أن التشفير السريع الآمن متاح للعامة على الإنترنت، حتى لو أدركوا بقدر ضئيل أنه موجود ويحمي مصالحهم. ويتعلق الأمر برمَّته بالأعداد، والأعداد الأولية في هذا الموضوع بالذات.

## كيف تحمي الأعدادُ الأولية السرية أسرارَنا؟

تذكَّرْ أن كلَّ رسالةِ نصٍّ عاديٍّ تُمثَّل بعدد واحد فحسب؛ لذا فمن الطبيعي محاولة إخفاء هذا العدد باستخدام أعداد أخرى. أكثر الطرق شيوعًا للقيام بذلك تكون باستخدام ما يطلق عليه عملية تشفير ريفيست وشامير وأدلمان، التي نُشرت في عام ١٩٧٨ عن طريق مبتكريها رون ريفيست وآدي شامير وليوناردو أدلمان. وفي هذه الطريقة، يتكون المفتاح الخاص بكل شخص من ثلاثة أعداد $p$ و$q$ و$d$، بحيث يكون $p$ و$q$ عددين أوليَّين (كبيرين للغاية) والمكون الثالث $d$ هو عدد التشفير السري لأليس، وسوف نشرح دوره في الوقت المناسب. تُقدم أليس للآخرين $n = pq$، وهذا ناتج عدديها الأوليَّين السريين، وعدد التشفير $e$ (الذي يكون عددًا صحيحًا عاديًّا، لا يرتبط بأي شكل من الأشكال بالثابت الخاص الذي يطلق عليه $e$ المذكور في الفصل الثاني).

إليك المثال البسيط التالي للتوضيح: لدى أليس العدد الأولي $p = 5$ والعدد الأولي $q = 13$ بحيث $n = 5 \times 13 = 65$. إذا حددتْ أليس عدد التشفير الخاص بها ليكون $e = 11$، إذن فسيكون مفتاحها العام $(n, e) = (65, 11)$. ولتشفير الرسالة $m$، يحتاج بوب فقط $n$ و$e$. مع ذلك، يتطلب فك تشفير الرسالة المشفرة $E(m)$ التي أرسلها بوب إلى أليس عددَ فكِّ التشفير $d$، الذي اتضح في هذه الحالة أنه $d = 35$، كما سنوضح بعد قليل. إن العمليات الرياضية التي تسمح بحساب $d$ تتطلب بأن يكون العددان الأوَّليان $p$ و$q$ معلومَين. في هذا المثال التوضيحي، بمعرفة أن $n = 65$، يمكن لأي شخص أن يكتشف سريعًا أن $p = 5$ و$q = 13$. مع ذلك، إذا كان العددان الأوليان $p$ و$q$ كبيرين للغاية (عادة ما يتكونان من مئات الخانات)، تصبح هذه المهمة مستحيلة عمليًّا لأي

نظام حاسوبي تقريبًا، على الأقل لفترة قصيرة معتدلة، على غرار أسبوعين أو ثلاثة أسابيع. بإيجاز، يعتمد نظام التشفير بطريقة عملية تشفير ريفيست وشامير وأدلمان على الحقيقة التجريبية التي تنص على أنه من الصعب للغاية إيجاد العوامل الأولية للعدد $n$ الكبير جدًّا جدًّا. أما الجزء الأروع الذي سنشرحه في بقية الفصل فيتمثل في تصميم طريقة يمكن من خلالها تشفير عدد الرسالة $m$ باستخدام العددين المعروفين علانيةً $n$ و$e$ فحسب، ولكن فك التشفير في الواقع يتطلب امتلاك العوامل الأولية للعدد $n$.

إليك طريقة العمل. ما يرسله بوب عبر الأثير ليس $m$ نفسه، وإنما العدد الباقي من قسمة $m^e$ على $n$. بعد ذلك يمكن لأليس استعادة $m$ من خلال أخذ هذا العدد الباقي $r$ وبالمثل حساب العدد الباقي من قسمة $r^d$ على $n$. تضمن الأساليب الرياضية الأساسية أن يكون الناتج لدى أليس هو الرسالة الأصلية $m$، التي يمكن حينها فك تشفيرها وتحويلها إلى نص عادي باستخدام النظام الحاسوبي لدى أليس. وبالطبع يحدث هذا الأمر على نحو مثالي خلف الكواليس بالنسبة لأي أليس وبوب حقيقيَّين.

يبدو أن الشيء الوحيد المهم حقًّا الذي تفتقده إيف هو عدد فك الشفرة $d$. إذا عرفتْ إيف هذا العدد يمكنها أن تفك شفرة الرسالة مثلها مثل أليس. ويبدو أن $d$ هو حل لمعادلة معينة. وحل هذه المعادلة سهل للغاية حاسوبيًّا، ويعتمد على خوارزميات إقليدس المنشورة في «كتب إقليدس» في عام ٣٠٠ قبل الميلاد. ليس هذا مكمن الصعوبة، إنما تتمثل الصعوبة في أنه ليس ممكنًا اكتشافُ المعادلة التي يجب حلها بالضبط ما لم تكن تعلم على الأقل أحد العددين الأوليَّين $p$ و$q$، وهذه هي العقبة التي تعوق إيف عن تحقيق هدفها.

يمكننا توضيح المزيد عن كيفية عمل هذه الأعداد المتضمنة في العملية؛ أولًا: توجد مشكلة واضحة بالفعل في مهمة بوب الأولى. فالعدد $m$ كبير، والعدد $n$ ضخم (يتكون تقريبًا من مائتي خانة) وحتى إذا لم يكن $e$ كبيرًا بهذا الحجم، فسيكون العدد $m^e$ كبيرًا للغاية أيضًا. وبعد حسابه، علينا قسمة $m^e$ على العدد $n$ للحصول على الباقي $r$، الذي يمثل النص المشفر. ربما يبدو أن الحسابات صعبة للغاية لدرجة لا تجعلها عملية. وينبغي أن نعي أنه بالرغم من قوة أجهزة الكمبيوتر الحديثة، فإن لها حدودًا. وعندما تتضمن الحسابات أعدادًا مرفوعة لقوة كبيرة للغاية، فإنها يمكن أن تتخطى قدرات أي نظام حاسوبي. ولا يمكننا بالتأكيد افتراض أن أي حسابات عملية نخضعها للكمبيوتر يمكن إجراؤها في فترة زمنية قصيرة.

الأمر المبشِّر بالنسبة لبوب هو أنه من الممكن إيجاد العدد الباقي المطلوب $r$ دون القيام بعملية قسمة مطولة على الإطلاق. في الواقع، تعتمد البواقي على البواقي فحسب، وإليك مثالًا لتوضيح المقصود. ما هما الرقمان الأخيران في العدد $7^{39}$؟ (هذا يعني: ما الباقي عند قسمة هذا الرقم على 100؟) لكي نجيب على هذا السؤال، ربما نبدأ في حساب القوى الأولى القليلة المرفوع إليها العدد 7: $(7^1 = 7)$، $(7^2 = 49)$، $(7^3 = 343)$، $(7^4 = 2,401)$، $(7^5 = 16,807)$ ... مع ذلك، سوف يتضح سريعًا أن الحجم الكامل لهذه الأعداد سيصعب التعامل معه قبل الاقتراب من العدد $7^{39}$. على الجانب الآخر، إذا حسبنا قوةً بعد أخرى، فسنجد نمطًا يظهر. والملاحظة الرئيسية هي أننا حينما نحسب القوى المتتالية، نجد أن الخانتين الأخيرتين من النتيجة تعتمدان فقط على الخانتين الأخيرتين في العدد السابق؛ إذ إنه عندما نقوم بالضرب، فإن الأرقام الموجودة في خانة المئات وما بعدها لا يكون لها تأثير على ما تنتهي إليه خانتا الآحاد والعشرات.

الأكثر من ذلك أنه نظرًا لأن ناتج $7^4$ ينتهي بالرقمين 01 في الخانتين الأخيرتين، فإن ناتج رفع العدد 7 للقوى الأربعة التالية سوف ينتهي بالأعداد 07، 49، 43، ثم 01 مرة أخرى. وهكذا، بينما نحسب القوى المتتالية، سوف يكرر نمط الخانتين الأخيرتين هذه الدورة الرباعية ببساطة مرارًا وتكرارًا. وبالعودة للسؤال المذكور سابقًا، نظرًا لأن $39 = 4 \times 9 + 3$، فسوف نمر خلال هذه الدورة تسع مرات ثم نأخذ ثلاث خطوات إضافية من أجل حساب الرقمين الموجودين في الخانتين الأخيرتين من ناتج $7^{39}$؛ ومن ثم فلا بد أن يكون 43.

ينجح هذا بوجه عام. لكي تجد الباقي عند قسمة العدد المرفوع لقوة ما $a^b$ على $n$ مثلًا، نحتاج فقط أن نأخذ الباقي $r$ عند قسمة $a$ على $n$ ونتتبع البواقي على حين نأخذ القوى المتتالية المرفوع إليها $r$. وعندما نعمل على الباقي $r$، الذي سيكون عددًا يتراوح بين صفر و$n - 1$، يقول علماء الرياضيات إننا نستنبط باقي القسمة على $n$، ونتخلص من أي مضاعفات لعدد $n$ قد تظهر؛ إذ إنها تترك باقيًا يساوي صفرًا عند قسمتها على $n$؛ ومن ثم لا يمكنها أن تسهم في قيمة الباقي المتناهي $r$.

ربما لا تزال تشك في أني قد تلاعبتُ بالأدلة عن طريق اختيار مثال تترك فيه قوةٌ صغيرةٌ للغاية باقيًا يساوي 1؛ في هذا المثال كان $7^4$ أكبر من مضاعف $n = 100$ بمقدار 1. مع ذلك، فهذا صحيح جزئيًّا فقط؛ إذ يتضح أنه إذا أخذنا أي عددين $a$ و$n$،

يكون القاسم المشترك الأعظم بينهما هو $1$ (نطلق على هذين العددين «عددين أوليَّين فيما بينهما»)، فإنه يوجد دائمًا قوة $t$؛ حيث $a^t$ تساوي $1$ عند قسمتها على $n$، بمعنى بقاء $1$ عند القسمة على $n$. ومن هذه النقطة، فإن بواقي القوى المتتالية تتبع دورة من الطول $t$. مع ذلك، يمكن أن يكون من الصعب التنبؤ بقيمة $t$، ولكن من المعروف أن $t$ يجب أن تساوي أو تكون أحد عوامل العدد الذي يُكتب عادة بالصورة $\phi(n)$؛ أيْ قيمة «دالة فاي» لأويلر.

والآن، ما هي $\phi(n)$؟ تُعرَّف بأنها عدد الأعداد حتى $n$ التي تكوِّن مع $n$ أعدادًا أولية فيما بينها. على سبيل المثال، إذا كان $n = 15$، فإن مجموعة الأعداد المقصودة هي $\{1, 2, 4, 7, 8, 11, 13, 14\}$، وتتضمن كل الأعداد حتى العدد 15، التي ليس لها عامل مشترك مع 15 (عدا العامل الحتمي 1). ونظرًا لأن هذه المجموعة تتضمن 8 عناصر، نرى أن $\phi(15) = 8$. لحسن الحظ، توجد طريقة أسهل لإيجاد $\phi(n)$ لا تستلزم وضع قائمة واضحة بكل الأعداد الصحيحة التي تكوِّن مع $n$ أعدادًا أولية فيما بينها ثم حساب عددها. فكما هي الحال مع كل الدوال ذات هذه الطبيعة، يمكن التعبير عن قيمتها من خلال عملية تحليل $n$ لعوامله الأولية. وبالفعل نحتاج فحسب لمعرفة العوامل الأولية للعدد $n$، لكي يمكن إيجاد $\phi(n)$ عن طريق ضرب $n$ في كل كسر $(1 - \frac{1}{p})$؛ حيث $p$ تمثل كل القواسم الأولية للعدد $n$. على سبيل المثال، العوامل الأولية للعدد 15 هي 3 و5؛ لذا الإجابة في هذه الحالة هي:

$$\phi\,(15) = 15 \times \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \times \frac{2}{3} \times \frac{4}{5} = 8,$$

وهي النتيجة نفسها التي حصلنا عليها مباشرةً من التعريف. وباستخدام هذه الطريقة، ربما ترغب في التحقق بنفسك من أن $\phi(100) = 40$، وهكذا — على سبيل المثال — يتبع ذلك أن $7^{40}$ تساوي $1$ عند قسمتها على $100$. مع ذلك، كما رأينا بالفعل، أقل قوة للعدد 7 يَنتج عنها باقٍ يساوي 1 ليست 40 وإنما القاسم 4 الخاص بها.

كل هذا يعطي إشارة إلى أن العدد الذي أرسله بوب إلى أليس — $m^e$ مقسومًا على $n$ — يمكن حسابه بالفعل دون جهد كبير من جانب كمبيوتر بوب. مع ذلك، فالأعداد المستخدمة في الواقع كبيرة للغاية؛ لذا يلزم مزيد من التوضيح لإظهار أنه يمكن التعامل معها. والقوى الكبيرة المستعملة في حساب $m^e$ باستخدام الكمبيوتر يمكن التعامل معها

على مراحل عن طريق عملية تُعرف باسم «رفع القوة الجبرية السريع». ودون الخوض في تفاصيل، تتضمن العمليةُ عملياتِ تربيعٍ وضرب متتالية للقوى من أجل الوصول إلى $m^e$ مقسومًا على $n$؛ حيث تقود الصيغة الثنائية للعدد $e$ الخوارزميةَ للوصول السريع للباقي المطلوب في خطوات قليلة نسبيًّا.

## إقليدس يوضح لأليس كيفية التوصل لعدد فك الشفرة

العدد الذي يفك الشفرة هو العصا السحرية لدى المتلقي التي تسمح له باستنباط الرسالة. يُختار هذا العدد $d$ على أساس أن يَترك ناتجُ $de$ باقيًا يساوي 1 عند القسمة على $\phi(n)$. ونظرًا لأن $n = pq$ هو ناتج ضرب عددين أوليَّين مختلفين، فإن قيمة $\phi(n) = pq(1 - \frac{1}{p})(1 - \frac{1}{q}) = (p-1)(q-1)$. ويتضح أنه يوجد دائمًا قيمة واحدة فقط للعدد $d$ في نطاق الأعداد وصولًا إلى $\phi(n)$ الذي يملك السمة المطلوبة.

يستطيع كمبيوتر أليس أن يجد $d$ باستخدام أداة جبرية عمرها أكثر من ٢٣٠٠ عام، وهي خوارزمية إقليدس التي سنشرحها بعد قليل. ويمكن لكمبيوتر إيف أيضًا أن يفعل الأمر نفسه إذا كان يَعرف فحسب المعادلةَ التي يجب حلُّها. مع ذلك، نظرًا لأن $p$ و$q$ لا يعلمهما إلا أليس، فكذلك أيضًا $(p-1)(q-1)$، ولا تَعرف إيف من أين ستبدأ.

إن وجود $d$ مضمون فقط إذا وُضع قَيْد بسيط معين على عدد التشفير $e$ (المعلَن). يجب أن تَضْمن أليس أن $e$ ليس لديه عامل أوَّلي مشترك مع $\phi(n)$. ويمكن فعل ذلك بسهولة تامة؛ حيث يمكن لأليس أن تَختبر قسمة $\phi(n)$ على أعداد أولية معينة؛ ومن ثم تتأكد من أن $e$ يفي بهذه المتطلبات دون كشف هوية $p$ و$q$. وفي الواقع، قيمة $e$ المستخدمة في أغلب الأحيان فعليًّا هي «عدد فيرما الأولي» الرابع $e = 65537 = 2^{16} + 1$؛ وهذه القيمة $2^{2^4} + 1$ لديها سمة نادرة على نحو خاص، وهي أنه من الممكن رسم مضلع منتظم بأضلاع $e$ باستخدام مسطرة وفرجار. مع ذلك، ترجع فائدته في التشفير إلى كونه عددًا أوليًّا كبيرًا باعتدال يتخطى مضاعفات 2 بمقدار 1 بالضبط، وهو ما يتوافق جيدًا مع عملية الرفع الجبري السريع المذكورة سابقًا.

وبالعودة إلى خوارزمية إقليدس، فإنها تبدأ بملاحظة أنه من الممكن إيجاد العامل المشترك الأعظم لأي عددين $a > b$ بالطرح المتتابع. (العامل المشترك الأعظم يُعرف أيضًا

باسم «القاسم المشترك الأعظم».) نلاحظ أن $r = a - b$ يتمتع بِسَمة أن أيَّ عامل مشترك بين أي عددين من الثلاثة أعداد $a$ و$b$ و$r$ سوف يكون أيضًا أحد عوامل العدد الثالث. على سبيل المثال، إذا كان $c$ عاملًا مشتركًا بين $a$ و$b$؛ حيث $a = ca_1$ و$b = cb_1$ مثلًا، نجد أن $r = a - b = ca_1 - cb_1 = c(a_1 - b_1)$؛ مما يمنحنا تحليلًا للعدد $r$ إلى عوامل أولية يتضمن القاسم $c$. على وجه الخصوص، العامل المشترك الأعظم للعددين $a$ و$b$ هو العامل المشترك الأعظم نفسه للعددين $b$ و$r$. ونظرًا لأن هذين العددين أصغر من $a$، فإننا نواجه الآن المشكلة نفسها ولكنها تنطبق على زوج من الأعداد الأصغر. وسوف يؤدي تكرار هذه الفكرة في النهاية إلى زوج يكون فيه العامل المشترك الأعظم بديهيًّا. (في الواقع، العددان الموجودان لدينا سوف يكونان في النهاية متطابقين؛ إذ إنه إن لم يكونا كذلك، يمكننا مواصلة الأمر باتخاذ خطوة أخرى؛ وقيمتهما المتطابقة ستكون هي العدد الذي نبحث عنه.)

على سبيل المثال، لإيجاد العامل المشترك الأعظم للعددين $a = 558$ و$b = 396$، فإن عملية الطرح الأولى سوف تعطينا $r = 558 - 396 = 162$؛ لذا فإن الزوج الجديد سيكون 396 و162. ونظرًا لأن $396 - 162 = 234$، فإن الزوج الثالث يصبح 234 و162، وعندما نواصل الطرح، ستكون القائمة الكاملة لأزواج الأعداد هي:

$$\begin{aligned}(558, 396) &\longrightarrow (396, 162) \longrightarrow (234, 162)\\ &\longrightarrow (162, 72) \longrightarrow (90, 72) \longrightarrow (72, 18)\\ &\longrightarrow (54, 18) \longrightarrow (36, 18) \longrightarrow (18, 18)\end{aligned}$$

ومن ثم فإن العامل المشترك الأعظم للعددين 558 و396 هو 18.

من الممكن كتابة العامل المشترك الأعظم لزوج من الأعداد، من تحليل العددين لعواملهما الأولية. في هذا المثال، $558 = 2 \times 3^2 \times 31$، بينما $396 = 2^2 \times 3^2 \times 11$؛ وبأخذ القوة المشتركة لكل عدد أولي داخل في عملية التحليل، نحصل على العامل المشترك الأعظم $18 = 2 \times 3^2$. مع ذلك، الأعداد الكبيرة تتطلب جهدًا أقل في استخدام خوارزمية إقليدس؛ إذ إن إجراء عمليات الطرح أسهل عمومًا من التحليل للعوامل الأولية.

توجد ميزة أخرى لخوارزمية إقليدس؛ وهي أنه من الممكن دائمًا العمل على نحو معاكس، ومن ثم التعبير عن العامل المشترك الأعظم في سياق العددين الأصليين. ولرؤية

تطبيق ذلك على الواقع في المثال السابق، من الأفضل ضغط الحسابات عندما يظهر العدد نفسه عدة مرات على مدار عملية الطرح، ويمثِّل هذا في معادلة واحدة كما يلي:

$$558 = 396 + 162$$

$$396 = 2 \times 162 + 72$$

$$162 = 2 \times 72 + 18$$

$$72 = 4 \times 18.$$

بدءًا من السطر الثاني حتى السطر الأخير، نستخدم الآن كل معادلة صغيرة للتخلص من البواقي الوسيطة، واحدًا تلو الآخر. وفي هذا المثال، عن طريق استخدام المعادلة قبل الأخيرة أولًا، ثم المعادلة السابقة لها، نحصل على:

$$18 = 162 - 2 \times 72 = 162 - 2 \times (396 - 2 \times 162)$$

$$= 5 \times 162 - 2 \times 396$$

وفي النهاية نستخدم المعادلة الأولى للتخلص من الباقي الوسيط الأول 162:

$$= 5 \times (558 - 396) - 2 \times 396 = 5 \times 558 - 7 \times 396 = 18.$$

إن القدرة على إجراء هذه العملية العكسية مهمة لأسباب تطبيقية ونظرية. وعلى نحو خاص، لإيجاد عدد فك الشفرة $d$ لأليس، نريد أن يفي $d$ بشرط أن يترك $de$ باقيًا يساوي 1 عند القسمة على $\phi(n)$. (من أجل الاختصار، سوف نشير إلى $\phi(n)$ برمز واحد هو $k$.) نستطيع الآن إدراك السبب في إصرارنا على أن يكون $e$ و$k$ عددين أوليَّين فيما بينهما — كما لو كان العامل المشترك الأعظم لهما هو 1 — فعندما نطبق خوارزمية إقليدس على زوج الأعداد $e$ و$k$، فإن الباقي المتناهي الذي يظهر هو 1 بالطبع. وعن طريق عكس الخوارزمية، سوف نعبِّر في النهاية عن 1 بصفته مزيجًا من $e$ و$k$، وبصفة خاصة سوف نجد أعدادًا صحيحة مثل $c$ و$d$؛ حيث $ck + de = 1$ أو بعبارة أخرى، $de = 1 - ck$؛ ومن ثم فإن $de$ سوف تترك باقيًا 1 عند القسمة على $k$.

هذه العملية البسيطة نسبيًّا سوف تُنتج عدد فك الشفرة $d$ الخاص بأليس: وربما لا تقع القيمة الأولية للعدد $d$ — الناتجة عن المعادلة — ضمن النطاق الممتد من 1

إلى $k$، ولكن إذا كانت تقع، فسوف نحصل في النهاية على العدد الفريد من نوعه $d$ — بجمع أو طرح أحد مضاعفات $k$ المناسبة — ضمن هذا النطاق الذي يتمتع بالسمة السحرية المتمثلة في أن $de$ يترك باقيًا يساوي 1 عند القسمة على $k$. (من السهل إثبات تفرُّد العدد $d$، ولكننا لن نستطرد في مزيد من الشرح هنا.) هذه هي طريقة حساب عدد فك الشفرة $d$؛ إذ يمكننا توضيح ذلك عن طريق العودة للمثال المذكور سابقًا؛ حيث $p = 5$ و$q = 13$؛ ومن ثم فإن $n = pq = 5 \times 13 = 65$. ولدينا $\phi(n) = (p-1)(q-1) = 4 \times 12 = 48$. تحدد أليس $e = 11$. ونظرًا لأن 11 و48 عددان أوليان فيما بينهما، فإن هذا يقع ضمن نطاق القواعد. ومن ثم فإن تطبيق خوارزمية إقليدس على $\phi(n) = k = 48$ و$e = 11$ يعطينا:

$$48 = 4 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

مما يؤكد أن العامل المشترك الأعظم بين $k$ و$e$ هو بالفعل 1. وبعكس الخوارزمية نحصل على:

$$1 = 4 - 3 = 4 - (11 - 2 \times 4) = 3 \times 4 - 11$$

$$= 3(48 - 4 \times 11) - 11 = 3 \times 48 - 13 \times 11.$$

هذا يعطي قيمة أولية للعدد $d = -13$ كحلٍّ للشرط بأن يترك $11d$ باقيًا يساوي 1 عند القسمة على 48؛ لذلك من أجل الحصول على قيمة موجبة للعدد $d$ ضمن النطاق المطلوب، نضيف 48 لهذا العدد كي نحصل على $d = 48 - 13 = 35$.

يعود السبب في نجاح العدد $d$ بالنسبة لأليس إلى الحساب المقياسي وإلى حقيقة أن $de$ يترك باقيًا يساوي 1 عند القسمة على $k = \phi(n)$. تحسب أليس $(m^e)^d = m^{de}$ مقسومًا على $n$. والآن يَتَّخذ العدد $de$ الصيغة $1 + kr$ بالنسبة للعدد الصحيح $r$. وكما ذُكر سابقًا، $m^k$ يترك باقيًا يساوي 1 عند القسمة على $n$ (يُعرف هذا عادة باسم «نظرية أويلر»)، وكذلك ينطبق الأمر نفسه على $(m^k)^r = m^{kr}$. ومن ثم فإن $m^{1+kr} = m \times m^{kr}$ يترك باقيًا يساوي $m$ عند القسمة على $n$. (التحقق المفصل من

هذه المعادلة يتطلب قليلًا من العمليات الجبرية، ولكن هذا هو ما يحدث.) بهذه الطريقة تستنبط أليس رسالة بوب؛ $m$.

وبالمناسبة، تجدر الإشارة إلى أن خوارزمية إقليدس تقدم الرابط المفقود في إثباتنا لتفرُّد عملية التحليل لعوامل أولية؛ حيث تسمح لنا بإثبات السمة الإقليدية بأنه إذا كان العدد الأولي $p$ أحدَ عوامل ناتج $ab$، بحيث $ab = pc$ مثلًا، فإن $p$ أحد عوامل $a$ أو $b$ على الأقل. السبب في ذلك هو أنه إذا لم يكن $p$ أحد عوامل $a$، فنظرًا لأن $p$ عدد أولي، فإن العامل المشترك الأعظم بين $p$ و$a$ هو 1. وعن طريق عكس خوارزمية إقليدس عند تطبيقها على الزوج $a$ و$p$، يمكننا إيجاد العددين الصحيحين $r$ و$s$ بحيث يكون مثلًا $ra + sp = 1$. وهذا يكفي لإيضاح أن $p$ أحد عوامل $b$؛ لأنه نظرًا لأن $ab = pc$، يكون لدينا:

$$b = b \times 1 = b(ra + sp) = r(ab) + psb$$

$$= r(pc) + psb = p(rc + sb).$$

هذه هي عملية تحليل العدد $b$ لعوامله الأولية، التي تبيِّن أن العدد الأولي $p$ أحد العوامل.

في الختام، إن نظرية الأعداد الكامنة وراء عملية تشفير ريفيست وشامير وأدلمان تجعل النظام سليمًا، مع أنه يجب مراعاة العديد من البروتوكولات التي لم أوضِّحها هنا من أجل الحفاظ على سلامة النظام. فهناك مشكلات «إثبات الهوية» (ماذا لو تواصلت إيف مع أليس على أنها بوب؟) و«عدم الإنكار» (ماذا لو تظاهر بوب أن إيف هي التي بعثتْ برسالته إلى أليس؟) و«انتحال الشخصيات» (ماذا لو أساءت أليس استخدام الهوية السرية التي أرسلها لها بوب وحاولَت انتحال شخصيته إلكترونيًّا؟) علاوة على ذلك، يمكن كشف مَوَاطن ضعفٍ أخرى في النظام عند انتشار رسائل يمكن التنبؤ بها أو رسائل متكررة. مع ذلك، فمن المحتمل أن تظهر هذه الصعوبات في أي نظام تشفير بالمفتاح العام، ويمكن التغلب عليها. وبصفة أساسية، لا علاقة لهذه الصعوبات بالأساليب الرياضية الأساسية التي تضمن الجودة العالية والتشفير القوي.

أَوْضَحَ هذا الفصلُ تطبيقًا رئيسيًّا للأعداد الأولية ونظريةَ قابليةِ القسمة والبواقي. وأَسْهمَت رياضيات إقليدس القديمة وكذلك إسهامات أويلر في القرن الثامن عشر في شرح ذلك، ليس من حيث المبدأ العام فحسب، وإنما أيضًا بالتفاصيل الدقيقة.

نختتم الجزء الأول من كتابنا بالفصل الخامس الذي سيقدِّم بعض الفئات الخاصة للأعداد الصحيحة المرتبطة بتعداد بعض التجميعات التي تَحْدث على نحوٍ طبيعي.

الفصل الخامس

# الأعداد المهمة

إنَّ الأعداد التي تظهر تلقائيًّا في مسائل العد مهمة؛ ولذلك خضعت لدراسات مكثفة. وسأشير هنا إلى معاملات ذات الحدَّين، والأعداد الكاتلانية، وأعداد فيبوناتشي، وأعداد سترلينج؛ لأنها تَسْرد مجموعات طبيعية معينة. ولكن سنبدأ أولًا بمتتاليات أعداد كبيرة الأهمية.

## الأعداد المثلثية والمتتالية الهندسية والمتتالية الحسابية

نظرًا لأننا سنعاود التطرق إلى الأعداد المثلثية لدى التحدث عن معاملات ذات الحدين، فسوف ألقي نظرة عليها الآن. فالعدد $n$ منها — ويُرمز له $t_n$ — يُعرَّف بأنه مجموع أول $n$ من أعداد العد. ويمكن تحديد قيمته — باستخدام صيغة $n$ — بالحيلة التالية؛ إذ نكتب $t_n$ بوصفها ناتج الجمع المذكور للتوِّ، ثم نكتبها مرة أخرى كنفس المجموع ولكن بترتيب معكوس. وعند جمع نسختَي $t_n$ معًا:

$$t_n = 1 + 2 + 3 + \cdots + (n-2) + (n-1) + n$$

$$t_n = n + (n-1) + (n-2) + \cdots + 3 + 2 + 1;$$

فإن الناتج بالطبع سيكون التعبير الجبري $2t_n$. مع ذلك، فالهدف من القيام بذلك هو اقتران 1 مع $n$، و2 مع $n-1$، و3 مع $n-2$، وهكذا. فمجموع أيٍّ من هذه الأزواج يعطي القيمة نفسها؛ وهي $n+1$، ويوجد $n$ من هذه الأزواج معًا. في النهاية، نستنتج أن $2t_n = n(n+1)$، أو بعبارة أخرى، قيمة $n$ في العدد المثلثي هي

$\frac{1}{2}n(n+1)$. على سبيل المثال، مجموع كل الأعداد الصحيحة من 1 حتى 1000 يساوي $500 \times 1001 = 500,500$.

في الواقع، تسمح لنا هذه المعادلة بإيجاد قاعدة لجمع أول $n$ من الحدود لأي متسلسلة حسابية، أو متتالية كما يطلق عليها، وتكون في صيغة $a, a+b, a+2b, a+3b, \ldots$. وعلينا أولًا أن ننتبه لتغيير المقدار. فمن خلال ضرب التعبير الجبري $t_n$ في $b$، نرى أن $b + 2b + 3b + \cdots + nb = \frac{b}{2}n(n+1)$. ولإيجاد معادلة حاصل جمع المتسلسلات الحسابية العامة، لاحظ أولًا أن حاصل جمع حدَّي $n-1$ الأولين في المتسلسلة السابقة ينتج عن طريق استبدال $n-1$ مكان $n$ في المعادلة السابقة، من أجل الوصول إلى $\frac{b}{2}n(n-1)$. وتنتج المتسلسلة الحسابية العامة الآن من إضافة $a$ لكل حد ووضع $a$ كأول حد أيضًا. وهذا يعني أننا نحتاج لإضافة $na$ إلى المجموع السابق للحصول على المعادلة العامة لحاصل جمع $n$ من الحدود الأولى في المتسلسلة الحسابية:

$$a + (a+b) + (a+2b) + \cdots + (a+(n-1)b)$$
$$= na + \frac{b}{2}n(n-1).$$

على سبيل المثال، بوضع $a = 1$ و$b = 2$، نجد أن حاصل جمع $n$ من الأعداد الفردية الأولى هو $n + n(n-1) = n + n^2 - n = n^2$، أي مربع $n$.

إذا استبدلنا الضرب بالجمع، ننتقل من المتسلسلة الحسابية إلى «المتسلسلة الهندسية». في المتسلسلة الحسابية، يُفرَّق بين كل زوج من الحدود المتتالية بـ «الفرق المشترك»، وهو العدد $b$ في نظام الترميز الذي نستخدمه. بعبارة أخرى، للانتقال من حد إلى الحد التالي، نضيف $b$ ببساطة. وفي المتسلسلة الهندسية، نبدأ مرة أخرى بعدد عشوائي، $a$ بوصفه الحد الأول، ثم ننتقل من حدٍّ إلى حدٍّ تالٍ عن طريق «الضرب» في عدد ثابت، يسمى «نسبة مشتركة»، ويُشار إليها بالرمز $r$. بمعنى أن المتسلسلة الهندسية العادية تكون في صورة $a, ar, ar^2, \ldots$ بحيث يكون الحد $n$ معادلًا للعبارة $ar^{n-1}$. وكما هي الحال مع المتسلسلة الحسابية، توجد معادلة لحاصل جمع أول $n$ من الحدود في المتسلسلة الهندسية:

$$a + ar + ar^2 + \cdots + ar^{n-1} = \frac{a(r^n - 1)}{r-1}.$$

الطريقة السريعة للتحقق من صحة هذه المعادلة هي الحصول على الطرفين المتساويين من ضرب كلا طرفي هذه المعادلة في $(r-1)$ والضرب خارج الأقواس. فنحصل من الجانب الأيسر على ما يلي:

$$(ar+ar^2+ar^3+\cdots+ar^n)-(a+ar+ar^2+\cdots+ar^{n-1}).$$

فيقصُر التعبير الجبري كله، بمعنى أنه كلُّ حدٍّ فيه تقريبًا يُلغى بواسطة حدٍّ في القوس الآخر: الاستثناء الوحيد هو $ar^n-a=a(r^n-1)$، مما يبين أن معادلتنا لناتج الجمع صحيحة. على سبيل المثال، بوضع $a=1$ و$r=2$، نحصل على ناتج جمع قوى العدد 2:

$$1+2+4+\cdots+2^{n-1}=2^n-1.$$

وهذه المعادلة هي ما تحتاجه فحسب من أجل التحقق من نتائج إقليدس في الفصل الثالث حول كيفية الحصول على أعداد كاملة زوجية من أعداد ميرسين الأولية.

## المضروب والتباديل ومعاملات ذات الحدين

كما رأينا سابقًا، العدد $n$ المثلثي ينشأ من جمع كل الأعداد من 1 حتى $n$ معًا. وإذا استبدلنا الضرب بالجمع في هذه الفكرة، فسنحصل على ما يسمى «أعداد المضروب»، التي سَبَقَت الإشارة إليها في الفصل الثاني.

يظهر المضروب باستمرار في مسائل العد والاحتمال؛ مثل احتمالات الحصول على مجموعة معينة من الأوراق في ألعاب الورق على غرار البوكر. ولهذا السبب، لديه رمزه الخاص؛ إذ يشار إلى المضروب $n$ بالمعادلة $n!=n\times(n-1)\times\cdots\times2\times1$. تتزايد الأعداد المثلثية بسرعة معقولة، إلى قرابة نصف معدل الأعداد المربعة، ولكن أعداد المضروب تتزايد بسرعة كبيرة، وسريعًا ما تتجاوز الملايين والملايين؛ على سبيل المثال $10!=3,628,800$. وتُنَبِّهُنا علامة التعجب إلى معدل نموِّها المخيف هذا.

وعلى وجه الخصوص، العدد $n!$ يمثل عدد الطرق المختلفة المميزة التي يمكنك من خلالها ترتيب $n$ من العناصر في صف؛ على غرار الكرات المرقمة البالغ عددها $n$. وهذا يتبع أنه لديك خيارات عددها $n$ لاختيار الكرة التي توضع في البداية، ولكل خيار من

هذه الخيارات لديك عدد $n-1$ من الكرات لتُوضع في المكان الثاني، و$n-2$ للمكان الثالث، وهكذا. وإذا توقفنا بعد اختيار كرات $r$ فحسب، وأشرنا إلى العدد المقابل لها بالعبارة $P(n,r)$، نرى أنه يوجد $n\times(n-1)\times(n-2)\times\cdots\times(n-r+1)$ من التباديل — كما قلنا — الخاصة بالكرات $n$، مع أخذ $r$ في كل مرة. يُعبَّر عن ذلك أيضًا على نحو مناسب بأنه النسبة بين عاملين: $P(n,r)=\frac{n!}{(n-r)!}$. على سبيل المثال، إذا كنت توزع دورة في لعبة البوكر، تأخذ خمس بطاقات من مجموعة الورق البالغ عددها 52، وعدد الطرق التي يمكن أن يحدث بها ذلك هي $P(52,5)=52\times51\times50\times49\times48$. مع ذلك، لا تعتمد دورة الورق في البوكر على ترتيب سحبك للبطاقات، ولكن على مجموعة الورق نفسها فحسب. فبالنسبة لدورة الورق، فإن كل خمس بطاقات يمكن أن يعاد ترتيبها بطرق يبلغ عددها $5!=120$؛ لذلك فإن عدد سحب البطاقات الخمس المختلفة حقًّا هو $P(52,5)/120=2,598,960$؛ أيْ حوالي مليونين ونصف مليون طريقة.

أكثر الفئات تميزًا التي تظهر في مسائل العد — أو كما يطلق عليها «السرد» — هي فئة «معاملات ذات الحدين»، وسميت هكذا لأنها تنشأ كمضاعفات لقوى $x$ عند فك التعبير الجبري ذي الحدين $(1+x)^n$. والمعامل ذو الحدين $C(n,r)$ هو عدد الطرق المختلفة التي قد نبني من خلالها مجموعة من الحجم $r$ من مجموعة من الحجم $n$. على سبيل المثال: $C(4,2)=6$؛ إذ إنه يوجد ستة أزواج (مأخوذة دون الوضع في الاعتبارِ الترتيبَ داخلَ الزوج) يمكن اختيارها من مجموعة من أربعة؛ على سبيل المثال: إذا كان لدينا أربعة أطفال — أليكس وباربرا وكارولين وديفيد — يوجد ست طرق يمكننا من خلالها اختيار زوجٍ من المجموعة: AB, AC, AD, BC, BD, CD.

يمكن حساب معاملات ذات الحدين بطريقتين مختلفتين؛ أولًا: يمكننا توسيع نطاق البرهان السابق الذي استخدمناه لحساب $C(52,5)$: فنرى بوجه عام أن $C(n,r)=P(n,r)/r!$، التي بدورها تقدم لنا التعبير الجبري المفيد:

$$C(n,r)=\frac{n!}{(n-r)!r!}.$$

وتحدث حالة خاصة بارزة عندما نضع $r=2$، تقابل عدد الأزواج التي يمكن اختيارها من مجموعة عناصر $n$. الجواب هو $\frac{n!}{(n-2)!2!}$. والآن، كل العوامل الموجودة في الحد $(n-2)!$ في المقام تُلغى مع العوامل المقابلة في $n!$، ونظرًا لأن $2!=2$، فإن التعبير $C(n,2)$ يُبسط إلى $\frac{n(n-1)}{2}$. بعبارة أخرى، عدد طرق اختيار زوج من مجموعة من

عناصر $n$ هو $t_{n-1}$، مع كون $(n-1)\text{st}$ عددًا مثلثيًّا. على سبيل المثال، كما رأينا بالفعل، $C(4,2)=6$، الذي هو بالفعل العدد المثلثي الثالث.

إنَّ هذه الصيغة القائمة على المضروب لحساب معاملات ذات الحدين تقدم بالفعل فهمًا جبريًّا تامًّا للمعاملات ذات الحدين؛ مما يمكِّننا من إيضاح خصائصها المميزة العديدة. مع ذلك، عادةً ما يكون تطوُّر هذه الخصائص أكثر وضوحًا إذا ركَّزنا على طريقة ثانية لإنتاج هذه الأعداد الصحيحة، وهي من خلال المثلث الحسابي (انظر شكل ٥-١)، المعروف أيضًا باسم مثلث باسكال، تكريمًا لعالم الرياضيات والفيلسوف الفرنسي بليز باسكال (١٦٢٣–١٦٦٢) الذي عاش في القرن السابع عشر. (اكتُشف المثلث الحسابي وأعيد اكتشافه في فارس والهند والصين على مدار الألفية السابقة: على سبيل المثال، كان موجودًا على الغلاف الأمامي لكتاب «المرآة النفيسة» الذي ألفه تشو شيه تشيه في عام ١٣٠٣.)

كل عدد في هيكل المثلث هو ناتج جمع العددين الموجودَين أعلاه. والمثلث — الذي يمكن مواصلة تكوينه إلى ما لا نهاية — يقدِّم قائمةً كاملة من معاملات ذات الحدين. على سبيل المثال، لإيجاد عدد الطرق التي يمكن من خلالها اختيار خمسة أشخاص من مجموعة بها سبعة أشخاص، اتَّبِع الخطوات التالية: رقِّم سطور المثلث بدءًا من صفر في القمة، وعلى نحو مماثل رقِّم المواضع في كل صف من اليسار إلى اليمين، بدءًا من صفر مرة أخرى، واذهب إلى السطر رقم 7، ثم اذهب للعدد الموجود في ذلك السطر في الموضع الخامس (تذكَّر أن تبدأ العد من صفر)؛ سنجد أن الإجابة هي 21. سوف تلاحظ تماثل كل صف؛ على سبيل المثال، 21 هو أيضًا عدد طرق اختيار شخصين من مجموعة فيها سبعة أشخاص. يُفسَّر ذلك من خلال ملاحظة أنه عندما نختار الخمسة من السبعة، فإننا في الوقت نفسه نختار اثنين من السبعة أيضًا؛ الاثنان هما الزوج المتبقي. وبرهان التماثل هذا ينطبق بالطبع على كل صف. وهذا أيضًا مبرهن عليه في المعادلة: $C(n,r)=\frac{n!}{(n-r)!r!}$؛ حيث إنها تعطينا التعبير نفسه إذا استبدلنا $n-r$ بـ $r$؛ إذ إن الحدين $r$ و$n-r$ اللذين نراهما في المقام يتبادلان فحسب مكانيهما.

ليس من الصعب إدراك السبب في أن هذا النمط يقدم الإجابة الصحيحة. فكل صف مبنيٌّ من الصف الموجود فوقه. ويمكننا أن نرى بسهولة أن الصفوف الثلاثة الأولى صحيحة: على سبيل المثال، العدد 2 في مركز الصف الثالث يعلمنا بأنه توجد طريقتان لاختيار شخص واحد من زوج من الأشخاص. والعدد 1 الموجود على القمة يقول إنه

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1 \\
1 \quad 8 \quad 28 \quad 56 \quad 70 \quad 56 \quad 28 \quad 8 \quad 1 \\
\vdots
\end{array}
$$

شكل ٥-١: المثلث الحسابي.

توجد طريقة واحدة لاختيار مجموعة بالحجم صفر من المجموعة الفارغة. وفي الواقع، توجد طريقة واحدة لاختيار مجموعة بالحجم صفر من أي مجموعة، وهذا هو السبب في بدء كل صف بالعدد 1. دعنا نركز على المثال المقدم للتو: توجد 21 $(6 + 15 = 21)$ طريقة لاختيار خمسة من مجموعة من سبعة أشخاص. تنقسم المجموعات الخماسية البالغ عددها 21 طبيعيًّا إلى نوعين. أولًا، توجد 15 طريقة لتكوين مجموعة من أربعة من أول ستة أشخاص، ويمكننا إضافة الشخص السابع لكلٍّ منها لتكوين مجموعة الخمسة أشخاص. مع ذلك، إذا لم نشمل الشخص السابع في ذلك، فعلينا حينها تكوينُ مجموعة من خمسة أشخاص من أول ستة أشخاص، وتوجد ست طرق للقيام بهذا الأمر. وهذا يوضح كيف يؤدي كل صف إلى الصف الذي يليه؛ فكل عنصر يمثل مجموع العنصرين الموجودين أعلاه، وهذا النمط هو السائد في المثلث. وبالرموز، تتخذ هذه القاعدة الشكل:

$$C(n,r) = C(n-1,r) + C(n-1,r-1).$$

والمثلث غني بالأنماط. على سبيل المثال، مجموع الأعداد في كل صف متتابع يعطي المتتالية المتضاعفة 1، 2، 4، 8، 16، 32 … متتالية قوى العدد 2. وعلى سبيل المثال، بجمع الصف الذي يبدأ 1، 8، 28، 56 … فإننا نجمع عدد طرق اختيار مجموعة بالحجم 0، 1، 2، 3 … من مجموعة من 8. وفي النهاية، يعطينا ذلك عدد طرق اختيار مجموعة بأي حجم من مجموعة من 8 عناصر، وهو ما يساوي ناتج $2^8$؛ وعمومًا مجموعة بالحجم $n$ تحتوي على $2^n$ من المجموعات الفرعية بداخلها.

يمكن رؤية هذه الحقيقة الأخيرة مباشرةً؛ إذ إنه يمكن تحديد مجموعة فرعية من مجموعة بالحجم $n$ من خلال سلسلة ثنائية بالطول $n$ بالطريقة التالية. نضع المجموعة المذكورة بترتيب معين $\{a_1, a_2, \ldots, a_n\}$ مثلًا، ثم تحدد سلسلة ثنائية بالطول $n$ مجموعة فرعية من خلال قول إن كل ظهور للعدد 1 في السلسلة يشير إلى وجود $a_i$ المقابل في المجموعة الفرعية المنشودة. على سبيل المثال، إذا كان $n = 4$، فإن السلسلتين 0111 و0000 تمثلان $\{a_2, a_3, a_4\}$ على الترتيب، وتمثلان المجموعة الفارغة. ونظرًا لأنه يوجد خياران لكل مُدخل في السلسلة الثنائية، فيوجد عدد $2^n$ سلسلة إجمالًا؛ ومن ثم $2^n$ مجموعة فرعية ضمن مجموعة بالحجم $n$.

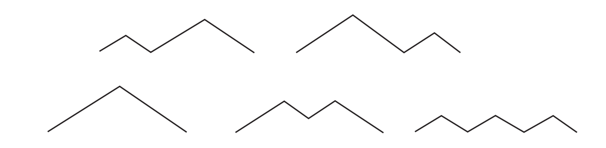
## الأعداد الكاتلانية

كل صف ثانٍ في المثلث الحسابي به عدد يقع في المنتصف: 1، 2، 6، 20، 70، 252، 924 ... وتقبل هذه الأعداد القسمة على أعداد العد المتتابعة 1، 2، 3، 4، 5، 6، 7 ... وتُعرف الأعداد التي تنتج من إجرائنا لعمليات القسمة تلك — 1، 1، 2، 5، 14، 42، 132 ... — باسم «الأعداد الكاتلانية». وباستخدام صيغة معاملات ذات الحدين المركزية تلك، يمكن التعبير عن العدد الكاتلاني $n$ بالعبارة الجبرية $\frac{1}{n+1}C(2n, n)$؛ حيث $n = 0, 1, 2, \ldots$.

أحد أبسط التمثيلات البصرية التي تُنتج هذا النوع من الأعداد هو عدد الطرق التي يُمْكننا من خلالها رسْمُ جبال باستخدام خطوط $n$ الصاعدة وخطوط $n$ النازلة (انظر شكل ٥-٢).

مع ذلك، فلكل نمط جبلي تفسير بوصفه آلية ذات معنًى للحصر داخل أقواس؛ ومن ثم فإن عدد الطرق ذات المعنى المستخدمة لترتيب مجموعة من أزواج الأقواس $n$ يعبِّر عن العدد الكاتلاني $n$. على سبيل المثال، الطريقتان ()(()) و((()))  هما طريقتان ذواتا معنًى للحصر داخل أقواس، ولكن الطريقة ())(() ليست ذات معنًى، ولكي تكون ذات معنًى، يجب ألا يقل عدد الأقواس المفتوحة إلى اليسار عن عدد الأقواس المفتوحة إلى اليمين حينما نعدُّ من اليمين إلى اليسار. وهذا يتوافق مع الشرط الطبيعي بأن جبالنا يجب ألا تغوص أسفل سطح الأرض. على سبيل المثال، يتوافق النمطان الجبليان الأول والأخير — في شكل ٥-٢ — مع آليَّتَي الحصر داخل الأقواس (())() و()()() على الترتيب.

كذلك يمثل العدد الكاتلاني $n$ عدد الطرق التي يمكننا من خلالها تقسيم مضلع منتظم بطول ضلع $n + 2$ إلى مثلثات عن طريق الخطوط القطرية التي لا تقطع بعضها بعضًا؛ ويوجد تفسيرات أخرى مصاحبة لهذه الخطوط. وكما هي الحال مع معاملات ذات الحدين، توجد معادلات تربط الأعداد الكاتلانية بأعداد كاتلانية أصغر، وهذا يجعلها قابلة للتلاعب بها.



شكل ٥-٢: بثلاثة خطوط صاعدة وثلاثة خطوط نازلة، يوجد خمسة أنماط جبلية.

## أعداد فيبوناتشي

متتالية فيبوناتشي هي متسلسلة من الأعداد التي تبهر العامة بشدة. وتسير المتتالية كما يلي:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, \ldots$$

حيث يكون كل عدد بعد عددَي 1 الأوَّلين هو مجموع العددين السابقين له. وفي هذا الأمر يوجد تشابُه مع معاملات ذات الحدين؛ حيث إن كل حد يكون مجموع الحدين السابقين له في المتتالية، ولكن طريقة تكوين أعداد فيبوناتشي أكثر بساطة:

$$f_n = f_{n-1} + f_{n-2}$$

حيث تشير $f_n$ إلى العدد فيبوناتشي $n$، ويُثبت $f_1 = f_2 = 1$. ونطلق على هذه الصيغة التي تحدد كل عنصر في المتتالية وفق سابقيه «تكرارًا» أو «علاقة تكرارية».

كيف تنشأ هذه المتتالية؟ قدَّمَها لأول مرة عام ١٢٠٢ ليوناردو أوف بيزا — الذي اشتُهر أكثر باسم فيبوناتشي — في صورة مسألة الأرنب الشهيرة الخاصة به. تولد أنثى

أرنب وبعد شهرين تصل إلى مرحلة النضج وتلد أرنبًا كل شهر. وعدد الأرانب الإناث الذي يكون لدينا في بداية كل شهر نتوصل إليه عن طريق أعداد فيبوناتشي؛ إذ إنه يوجد أنثى واحدة في بداية الشهر الأول والشهر الثاني، ولكن في بداية الشهر الثالث تلد الأنثى أرنبًا أخرى؛ ومن ثم يكون لدينا أنثيان. وفي الشهر اللاحق تلد أنثى أخرى، فيكون لدينا ثلاث، وفي الشهر الذي يليه يكون لدينا خمس أرانب؛ لأن الأم وكبرى بناتها قادرتان الآن على الإنجاب. وبوجه عام، في بداية كل شهر منذ ذلك الحين فصاعدًا، يكون عدد الإناث المولودات حديثًا مساويًا لعدد الإناث التي كانت لدينا قبلها بشهرين؛ حيث تكون قد كبرت بما يتيح التكاثر. يترتب على ذلك أن عدد الإناث لدينا في بداية كل شهر تالٍ يساوي مجموع الشهر السابق (أرانب فيبوناتشي خالدة) والعدد الذي لدينا في الشهر السابق له. ومن ثم، فإن قاعدة تكوين أعداد فيبوناتشي تتطابق تمامًا مع نمط التكاثر لدى هذه الأرانب.

وعلى الرغم من حقيقة أن الأرانب الحقيقية لا تتكاثر بهذه الطريقة المفتعلة، فإن أعداد فيبوناتشي تظهر في الطبيعة بمجموعة متنوعة من الطرق، بما في ذلك نمو النبات. وأسباب هذا الأمر مفهومة جيدًا، ولكن ترتبط بسمات أكثر دقة للمتتالية المرتبطة بما يسمى «النسبة الذهبية»، وهي العدد الذي نوشك على شرحه.

أبسط أنواع متتاليات الأعداد هي المتتاليات الحسابية والمتتاليات الهندسية المذكورتان في الجزء الأول. ومع أن متتالية فيبوناتشي ليست من أي النوعين، فإن لها مع ذلك رابطًا مدهشًا مع النوع الثاني. إذا شكَّلْنا متتالية فروق من متتالية فيبوناتشي، نحصل على 0، 1، 1، 2، 3، 5، 8، 13 ... استنادًا إلى طريقة تحديد المتتالية؛ أي إننا نستعيد متتالية فيبوناتشي مرة أخرى غير أننا نبدأ في هذه المرة من الصفر. يحدث هذا بالتحديد بسبب طريقة تكوين المتتالية: فالفارق بين عددي فيبوناتشي متتالين هو العدد الذي يسبقهما مباشرة في المتتالية. (لرؤية ذلك جبريًّا، اطرح $f_{n-1}$ من كلا طرفي تكرار فيبوناتشي السابق.) وليست المتتاليةُ متتاليةً هندسية؛ حيث إن النسبة بين عددي فيبوناتشي متتالين ليست ثابتة. مع ذلك، عندما ننظر للنسبة بين حدين متتالين، نرى أنها تستقر عند قيمة نهائية. ويظهر هذا السلوك شبه المستقر سريعًا إلى حدٍّ ما؛ حيث نجد عند قسمة كل عدد فيبوناتشي على سابقه:

$$\frac{34}{21} = 1.6190, \frac{55}{34} = 1.6176, \frac{89}{55} = 1.6182, \frac{144}{89} = 1.6180, \ldots$$

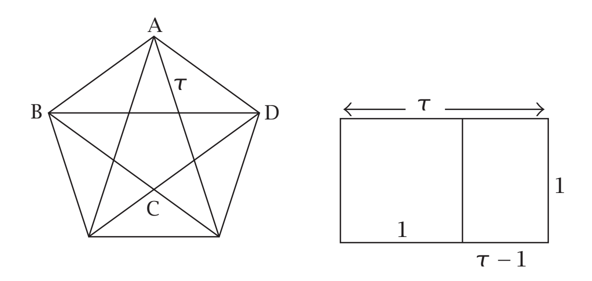
ولكن ما هذا العدد الغامض ...1.6180 الذي ينتج؟ هذا العدد $\tau$ يُعرف باسم النسبة الذهبية، ويظهر تلقائيًّا في السياقات الهندسية التي تبدو بعيدة كل البعد عن أرانب فيبوناتشي. على سبيل المثال، $\tau$ هي نسبة قطر المضلع الخماسي المنتظم إلى طول ضلعه (انظر شكل ٥-٣). وكل قطر يقابل آخر في نقطة تقسمه إلى جزأين النسبة بينهما هي $\tau : 1$. وأزواج الأضلاع المتقاطعة والأقطار المتقاطعة تشكل الأضلاع الأربعة للمعين (متوازي أضلاع «مربع») $ABCD$ كما هو موضح. عندما تتقاطع الأقطار، تُشَكِّل مضلعًا خماسيًّا أصغر مقلوبًا.

إن «التشابه الذاتي» من الخصائص المرتبطة بالنسبة الذهبية، ومعناه أن الأشكال — على غرار المضلع الخماسي — التي تتضمن $\tau$ عادة ما تحتوي داخلها على نسخ أصغر من نفسها. ويتضح هذا في المستطيل ذي الأضلاع التي يبلغ طولها $\tau$ و1؛ إذ إنه فريد من نوعه في عرض هذه السمة؛ فإذا اقتطعنا منه أكبر مربع يمكننا اقتطاعه (مربع طول ضلعه 1) فإن المستطيل الأصغر الذي يتبقى يكون نسخة من المستطيل الأصلي. وهذا الشكل يعرف بسبب ذلك باسم «المستطيل الذهبي» (انظر شكل ٥-٣). يمكن اكتشاف قيمة $\tau$ من السمة المذكورة للمستطيل؛ حيث إنه إذا سمَّيْنا طول الضلع الأطول $\tau$ وجعلنا الضلع الأقصر وحدة واحدة، نتوصل إلى التشابه بين المستطيلين من خلال المساواة بين $\frac{\tau}{1} = \frac{1}{\tau-1}$، التي نحصل عليها عن طريق مساواة النسبة بين الضلع الأطول والضلع الأقصَر في المستطيلين. وينتج عن الضرب التبادلي الذي يحدث في هذا التعبير الجبري، المعادلة $\tau^2 - \tau = 1$. وعند استخدام الصيغة العادية لحل هذه المعادلة التربيعية (المعادلة التي تتضمن عددًا مربعًا)، نجد أن الجذر الموجب لهذه المعادلة يساوي:

$$\tau = \frac{1+\sqrt{5}}{2} = 1.6180229\ldots$$

توجد طريقة أخرى لاستعادة قيمة $\tau$ من خلال ما يطلق عليه الكسر المستمر، الذي يربط $\tau$ مباشرة بأعداد فيبوناتشي، وسوف نشرح هذه الفكرة في الفصل السابع.

على المدى الطويل، تتصرف متتالية فيبوناتشي كأي متتالية هندسية معتمدة على النسبة الذهبية. وهذه السمة إضافة إلى قاعدة تكوينها البسيطة هما اللتان تجعلان متتالية فيبوناتشي تظهر على نحو مستمر.



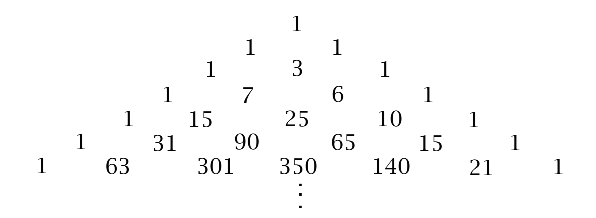

شكل ٥-٣: المضلع الخماسي والمستطيل الذهبي.

## أعداد سترلينج وأعداد بيل

تظهر أعداد سترلينج غالبًا في مسائل العد، وتعتمد على متغيرين $n$ و$r$ مثلها في ذلك مثل معاملات ذات الحدين. وعدد سترلينج $S(n,r)$ هو عدد طرق تقسيم عناصر المجموعة $n$ إلى كتل $r$ (بحيث لا تكون أي كتلة فارغة، ولا يكون ترتيب الكتل والترتيب داخل الكتل مُهمَّين). (وتسمى هذه الأعداد على وجه الدقة أعداد سترلينج من النوع الثاني. أما أعداد سترلينج من النوع الأول — المرتبطة — فتمثل شيئًا مختلفًا تمامًا، وهو عدد الطرق التي نستطيع من خلالها تبديل ترتيب عناصر $n$ في عدد $r$ دورة.) على سبيل المثال، المجموعة التي تحتوي على العناصر $a$ و$b$ و$c$ يمكن تقسيمها إلى ثلاث كتل بطريقة واحدة فقط: $\{a\}$، $\{b\}$، $\{c\}$، وإلى كتلتين بثلاث طرق: $(\{a,b\}$، $\{c\})$؛ $(\{a\}$، $\{b,c\})$؛ $(\{a,c\}$، $\{b\})$، وإلى كتلة واحدة بطريقة واحدة فقط: $\{a,b,c\}$؛ وينتج عن ذلك أن $S(3,1) = 1$، و$S(3,2) = 3$، و$S(3,3) = 1$. ونظرًا لأن المجموعة التي تحتوي على عناصر $n$ يمكن تقسيمها بطريقة واحدة إما إلى كتلة واحدة وإما إلى كتل $n$، فإنه يكون لدينا دائمًا $S(n,1) = 1 = S(n,n)$. وإذا رسمنا مثلث أعداد سترلينج باتباع طريقة مثلث باسكال، فسوف نحصل على منظومة الشكل ٥-٤، وسوف نشرح الآن كيفية تكوين المثلث.

مرة أخرى، تتَّبع الأعداد علاقة تكرار؛ مما يعني أن كلًّا منها يمكن ربطه بالأعداد السابقة له في المنظومة. وفي الواقع، كما هي الحال مع معاملات ذات الحدين، يمكن الحصول على كل عدد سترلينج من العددين الموجودين أعلاه، ولكنها ليست عملية

جمع بسيطة. علاوة على ذلك، تَماثُل الصفوف الذي نراه في المثلث الحسابي الذي يُنتج معاملات ذات الحدين ليس موجودًا في مثلث سترلينج. على سبيل المثال $S(5,2) = 15$ ولكن $S(5,4) = 10$. مع ذلك، فقاعدة التكرار بسيطة للغاية. على سبيل المثال، العنصر 90 يساوي $25 \times 3 + 15$. وهذا مؤشر على الموقف العام: فلإيجاد عدد في هيكل المثلث، خذ العددين الموجودين أعلاه مباشرةً، وأضِفِ الأول إلى الثاني مضروبًا في رقم موقع العدد — المطلوب إيجاده — في الصف. (وهذه المرة — على النقيض من المثلث الحسابي — ابدأ العد في الصف من 1.) وبالطريقة نفسها، العنصر $S(5,4) = 10 = 6 + 4 \times 1$. وجزء القاعدة الموضح بين قوسي التنصيص هو فقط الجزء الذي يختلف عن قاعدة المثلث الحسابي. ومع ذلك، يكفي هذا الجزء لجعل دراسة أعداد سترلينج أكثر صعوبة على نحو كبير من دراسة معاملات ذات الحدين. على سبيل المثال، لقد اشتققنا صيغة واضحة وبسيطة لكل معامل ذي حدين باستخدام صيغة المضروب. وعلى نحو مشابه، توجد صيغة لعدد فيبوناتشي $n$ باستخدام صيغة قوى النسبة الذهبية، ولكن لا يوجد صيغة من هذا النوع لأعداد سترلينج.




شكل ٥-٤: مثلث سترلينج.

ليس من الصعب شرح قاعدة التكرار؛ إذ كما نستخدم التكرار، نستخدم معاملات ذات الحدين. وبالقيام بذلك، نستعيد عملية التكرار المذكورة سابقًا التي تتطابق في الشكل فيما عدا وجود مضاعف وحيد. ومن أجل تقسيم مجموعة من الحجم $n$ إلى كتل $r$ غير فارغة، ربما نفعل ذلك عبر طريقتين مختلفتين. ربما نأخذ العناصر الأولى $n - 1$ من المجموعة ونقسمها إلى كتل $r - 1$ غير الفارغة باستخدام $S(n-1, r-1)$ طرقًا، والعنصر الأخير في المجموعة سوف يشكل حينها الكتلة $r$. وبدلًا من ذلك، ربما

نقسم عناصر $n-1$ الأولى من المجموعة إلى كتل $r$ غير الفارغة، باستخدام $S(n-1,r)$ طرقًا، ونقرر بعدها أي كتلة $r$ سنضع فيها العنصر الأخير من المجموعة، مانحين مضاعف $r$ إلى ذلك العدد. ومن ثم نستنتج أن:

$$S(n,r) = S(n-1,r-1) + rS(n-1,r)$$

عند $n = 2, 3, \ldots$

وباستخدام صيغة التكرار تلك، يمكننا حساب كل صف من مثلث سترلينج من الصف السابق له. على سبيل المثال، عند وضع $n = 7$ و$r = 5$، نحصل على:

$$S(7,5) = S(6,4) + 5S(6,5) = 65 + 5 \times 15 = 65 + 75 = 140.$$

يمكننا حساب $S(n,2)$ و$S(n,n-1)$ مباشرة من التعريف كما يلي: يُعبر عن التقسيم العشوائي للمجموعة $n$ إلى مجموعة أولى وثانية من خلال سلسلة ثنائية يبلغ طولها $n$؛ حيث يشير وجود 1 إلى الوجود في المجموعة الأولى، ووجود 0 إلى الوجود في المجموعة الثانية (بطريقة مشابهة لطريقة توضيحنا أن عدد المجموعات الفرعية للمجموعة $n$ هو $2^n$). ومن ثم يوجد $2^n$ أزواج مجموعات مرتبة. مع ذلك، نظرًا لأنه لا يوجد ترتيب للكتل داخل التقسيم، نقسم هذا العدد على 2 لنصل إلى عدد تقسيمات المجموعة $n$ إلى مجموعتين؛ ما ينتج عنه العدد $2^{n-1}$. وأخيرًا، علينا أن نطرح 1 من هذا العدد لكي نستبعد الحالة التي تكون فيها إحدى المجموعتين فارغة؛ ومن ثم، فإن $S(n,2) = 2^{n-1} - 1$. ويمكنك التحقق من أن هذه الصيغة تمثل الخط القطري الثاني للأعداد 1، 3، 7، 15، 31، 63 ... بدءًا من أعلى ناحية اليمين متوجهًا نحو الأسفل ناحية اليسار في الشكل ٥-٤.

على الطرف الآخر، يتحدد تقسيم المجموعة $n$ إلى كتل $n-1$ عن طريق اختيار الكتلة الفريدة ذات الحجم 2. وعدد طرق القيام بهذا الاختيار هي $C(n,2) = \frac{1}{2}n(n-1)$، العدد المثلثي رقم $(n-1)$. (انظر القطر الثاني 1، 3، 6، 10، 15، 21 ... المتجه من أعلى ناحية اليسار نحو الأسفل ناحية اليمين في الشكل ٥-٤.)

إن مجموع أي صف في المثلث الحسابي يعطي القوة للعدد 2؛ أي عدد المجموعات الفرعية لمجموعة ذات حجم معين. وعلى نحو مشابه، مجموع صف $n$ في مثلث سترلينج يعطي عدد طرق تقسيم مجموعة من عناصر $n$ إلى كتل، ويُطلق على هذا العدد «عدد بيل $n$».

## أعداد التجزئة

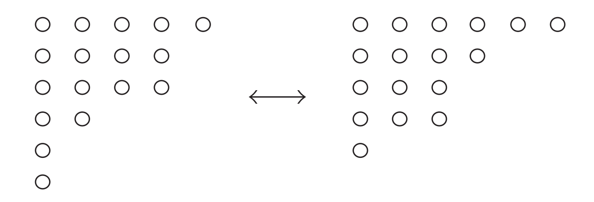
على الجانب الآخر، إذا كانت عناصر $n$ في المجموعة التي ستُجزأ متطابقة — ومن ثم لا يمكن التمييز بينها — فإن عدد طرق تقسيم المجموعة بأكملها إلى كتل هو عدد صحيح أصغر كثيرًا من الأعداد السابقة؛ وهو يُعرف باسم «عدد التجزئة $n$». ويُعبر عن أعداد التجزئة بكتابة $n$ بوصفها مجموع الأعداد الصحيحة، دون النظر إلى الترتيب: على سبيل المثال، $1 + 1 + 1 + 1 + 1$ هو تجزيء واحد من تجزيئات 5، ويوجد ستة آخرون؛ إذ يمكننا تمثيل 5 هكذا: $2 + 1 + 1 + 1$، أو $2 + 2 + 1$، أو $3 + 1 + 1$، أو $3 + 2$، أو $4 + 1$، أو ببساطة 5. ومن ثم فإن عدد التجزئة الخامس هو 7 (وذلك مقارنة بعدد بيل الخامس، الذي ندرك من مثلث سترلينج أنه $52 = 1 + 10 + 25 + 15 + 1$). ولا توجد صيغة دقيقة بسيطة لعدد التجزئة $n$؛ وإنما توجد صيغة معقدة، تعتمد هي نفسها على تقريب حسن يُنسب للعبقري الهندي سرينيفاسا رامانوجان (١٨٨٧–١٩٢٠).

أحد أوجُه التماثل البسيطة في أعداد التجزئة هو أن عدد تجزيئات $n$ إلى أجزاء $m$ يساوي عدد تجزيئات $n$ التي يكون فيها الجزء الأكبر $m$. إحدى الطرق للتحقق من صحة ذلك عن طريق رسم فيرار البياني (أو «مخطط يونج») لعدد التجزئة؛ وهو مجرد تمثيل لعدد التجزئة كمنظومة متطابقة من النقاط، والتي تُدرج فيها الصفوف بحجم متناقص.

في المثال الموضح في الشكل ٥-٥، مثَّلنا العدد 17 مجزأً إلى 1+1+2+4+4+5. لاحِظْ كيف أُدرجت الأعمدة أيضًا بترتيب تنازلي من اليسار إلى اليمين. وإذا عكسنا المنظومة على الخط القطري الممتد من أعلى ناحية اليسار إلى أسفل ناحية اليمين، نستعيد رسم فيرار آخر كما هو موضح، والذي يمكن تفسيره كعدد التجزئة $1 + 3 + 3 + 4 + 6 = 17$. وانعكاس مشابه للرسم الثاني يعود بك إلى الرسم الأول؛ ولذا نقول إن عددَي التجزئة المتطابقين يمثلان ثنائيًّا يماثل أحدهما الآخر. هذا التماثل يساعدنا على إدراك أن أعداد تجزئة نوعين متطابقين متساوية؛ فثنائي عدد التجزئة الذي يكون فيه $m$ مثلًا أكبر عدد (حيث يحتوي الصف الأعلى على $m$ من النقاط) هو تجزيء يحتوي على $m$ من الصفوف، ويتطابق مع تجزيء إلى $m$ من الأعداد. على سبيل المثال، عدد تجزيئات 17 إلى 6 أعداد يساوي عدد تجزيئات 17 التي يكون فيها 6 هو أكبر الأعداد الموجودة.

ينتبه علماء الرياضيات دومًا لهذا النوع من التماثل الذي يظهر غالبًا في مسائل العد. ونرى مثالًا آخر على ذلك يرتبط بمسألة اقتراع برتراند–وإيتوورث حيث تُفرز

الأصوات لاثنين من المرشحين ويأخذ الفائز $p$ من الأصوات والخاسر $q$ من الأصوات على سبيل المثال. ويوضح البرهان الهندسي الذكي باستخدام ما يطلق عليه «مبدأ الانعكاس» أن حجم الأصوات حينما يتصدر الفائز الفرز خلال الليلة يساوي الهامش الأخير للفوز مقسومًا على عدد الأصوات كلها: $\frac{p-q}{p+q}$. وهذا بدوره يساوي حجم الأصوات حينما لا يتحقق هامش الفوز النهائي أبدًا حتى يُعد آخر صوت. والسبب في أن هذين العددين يجب أن يكونا متساويين هو أن نوعي العد يمثلان ثنائيًّا يماثل أحدهما الآخر في أن عكس ترتيب الأصوات في العد من النوع الأول يعطي عدًّا من النوع الثاني، والعكس بالعكس.



شكل ٥-٥: ثنائي عدد التجزئة $1 + 3 + 3 + 4 + 6 = 1 + 1 + 2 + 4 + 4 + 5 = 17$.

## أعداد هيل ستون

مع أن أعداد هيل ستون ليست أداة للعد، فإنها مثيرة للاهتمام؛ إذ إنها تتحدد أيضًا على نحو متكرر وتشبه في طبيعتها متتاليات القواسم الكاملة التي رأيناها في الفصل الثالث. والمسألة التالية أُطلق عليها العديد من الأسماء: «خوارزمية كولاتز»، أو «مسألة سيراكيوز»، أو في بعض الأحيان مسألة $3n + 1$، وهي ببساطة عبارة عن ملاحظة أنه عند البدء بالعدد $n$ يبدو أن العملية التالية تنتهي دومًا بالعدد 1. فإذا كان $n$ عددًا زوجيًّا، فاقسمه على 2، في حين إذا كان $n$ عددًا فرديًّا، فاستبدل به $3n + 1$. على سبيل المثال، عند البدء $n = 7$، تقودنا القواعد إلى المتتالية الآتية:

$$7 \longrightarrow 22 \longrightarrow 11 \longrightarrow 34 \longrightarrow 17 \longrightarrow 52 \longrightarrow 26 \longrightarrow 13 \longrightarrow 40$$

$$\longrightarrow 20 \longrightarrow 10 \longrightarrow 5 \longrightarrow 16 \longrightarrow 8 \longrightarrow 4 \longrightarrow 2 \longrightarrow 1.$$

ومن ثَم الحدسية صحيحة لعدد $n = 7$، وبالفعل تم التحقق من صحتها لكل الأعداد $n$ حتى لما يتجاوز مليون مليون. وتختلف الأمور إذا عبثتَ بالقواعد: فعلى سبيل المثال، عند استبدال $3n - 1$ بالقاعدة الأصلية $3n + 1$، تنتج الدورة:

$$7 \longrightarrow 20 \longrightarrow 10 \longrightarrow 5 \longrightarrow 14 \longrightarrow 7 \longrightarrow \cdots$$

تتصرف متتالية الأعداد التي تنتج عن هذه الحسابات مثل البَرَد (وبالإنجليزية هيل ستون، وتعني: قطع الثلج الصغيرة)؛ إذ إنها تزداد وتقل على نحو غير منتظم لفترة طويلة، ولكن يبدو في النهاية أنها ترتطم بالأرض. ومن بين أول ألف عدد صحيح، يصل أعلى عدد هيل ستون لدى أكثر من 350 عددًا منها إلى 9232 قبل الانهيار وصولًا إلى 1. وسوف يحدث ذلك عندما تصل إلى أحد مضاعفات العدد 2؛ حيث إنها هي الأعداد التي تسبب السقوط المباشر لمستوى الأرض دون مقابلة أي ارتفاعات أخرى.

ويمكن تمييز كل أنواع السمات المثيرة للاهتمام في الرسومات البيانية والمخططات المعتمدة على متتالية هيل ستون التي تذكِّرنا بالأنماط الفوضوية الأخرى التي تَظهر في الرياضيات والفيزياء. وإذا بحثتَ عن أعداد هيل ستون في محرك البحث المفضل لديك، فسوف تجد كثيرًا من المعلومات المثيرة في أغلب الأحيان، والقائمة على التخمينات في أحيان أخرى، ولكنها في الغالب غير حاسمة.

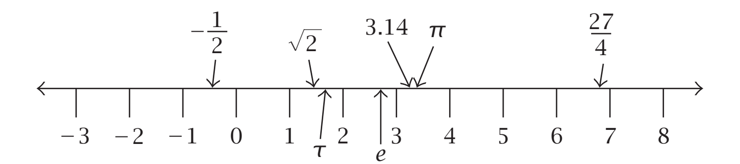
الفصل السادس

# ما وراء أعداد العد

## مقدمة

إن أعداد العد 1، 2، 3 ... هي فقط جزء صغير في منظومة الأعداد الأوسع نطاقًا. هذا الجزء هو بالطبع أول جزء استكشفناه، ولبعض الوقت ربما نظن أنه لا يوجد سواه في منظومة الأعداد، لا سيما إذا ظَلِلْنا عازفين عن النظر إلى ما وراءه. وخلال هذا الفصل، سوف نتناول أولًا الأعداد الصحيحة السالبة، وبالتعمق للوصول إلى الكسور — الموجبة والسالبة — نجد المجموعة التي يُطلَق عليها الأعداد النسبية. وعادةً ما تُرسم مجموعة الأعداد هذه على طول خط الأعداد؛ بحيث تقع الأعداد الموجبة على يمين الصفر، وتكوِّن الأعداد السالبة الصورة المقابلة لها على اليسار. مع ذلك، اتضح أن خط الأعداد هو موطن للأعداد الأخرى التي لا يمكن التعبير عنها في صورة كسور؛ مثل $\sqrt{2}$ و$\pi$. يطلق اسم «الأعداد الحقيقية» على كل الأعداد الموجودة على خط الأعداد، وهي تلك الأعداد التي يمكن تمثيلها عشريًّا (بالمفكوك العشري) من أي نوع، كما هو موضح في الشكل ٦-١.

مع ذلك، كان أحد أعظم إنجازات القرن التاسع عشر الإدراك التام بأن نطاق الأعداد الحقيقي ليس أحاديَّ البعد ولكنْ ثنائيَّ البعد. ومستوى الأعداد المركبة هو النطاق الطبيعي للنقاش في قدر كبير من علوم الرياضيات. وقد ظهر هذا النطاق للرياضيين والعلماء من خلال حل المسائل؛ فلِكَي تكون قادرًا على إجراء التحقيقات اللازمة لحل مسائل العالم الحقيقي — التي يبدو كثيرٌ منها متعلقًا بأعداد العد العادية — يصبح من الضروري توسيع أفق التفكير في الأعداد لديك. وتفسير كيفية ظهور هذا البعد الإضافي سوف يأتي في نهاية هذا الفصل وسيُشرح بعمق في الفصل الثامن.




شكل ٦-١: الجزء المركزي لخط الأعداد بالقرب من الصفر.

## الجمع والطرح

مصطلح الأعداد الصحيحة يطلق على مجموعة الأعداد كلها، موجبة وسالبة، والصفر. وهذه المجموعة — التي يرمز لها غالبًا بالرمز **Z** — ليس لها نهاية في الاتجاهين كليهما:

$$\{\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}.$$

وغالبًا ما تُصور الأعداد الصحيحة بوقوعها على نقاط بينها مسافات متساوية على خط الأعداد الأفقي، بالترتيب المبين سابقًا. والقواعد الإضافية التي نحتاج إلى معرفتها من أجل القيام بالعمليات الحسابية على الأعداد الصحيحة يمكن تلخيصها على النحو التالي:

(أ) لجمع أو طرح عدد صحيح سالب، $-m$، نتحرك مسافات مساوية للعدد $m$ نحو اليسار في حالة الجمع، ومسافات مساوية للعدد $m$ نحو اليمين من أجل الطرح.

(ب) لضرب عدد صحيح في $-m$، نضرب العدد الصحيح في $m$ ثم نغير العلامة.

بعبارة أخرى، اتجاه جمع وطرح الأعداد السالبة هو عكس اتجاه جمع وطرح الأعداد الموجبة، في حين ضَرْبُ عددٍ ما في $-1$ يغيِّر علامته إلى العلامة الأخرى. على سبيل المثال: $-3 = (-11) + 8$ و$-24 = (-8) \times 3$ و$1 = (-1) \times (-1)$.

يجب ألا تُواجِه أية مشكلة مع العملية الحسابية الأخيرة. أولًا: من المنطقي أنَّ ضَرْب عدد سالب في عدد موجب يُنتج إجابة سالبة: عندما تُفرض فائدة (مضاعف موجب أكبر من 1) على دَينٍ ما (عدد سالب)، فإن الناتج يكون دَينًا أكبر؛ أي عددًا سالبًا أكبر. جميعنا مدركون تمامًا لهذا الأمر. ويبدو متَّسِقًا أيضًا أن تؤدي عمليةُ ضَرْب عدد سالب

في عدد سالب آخر إلى النتيجة العكسية؛ أيْ نتيجة موجبة. ويمكن بسهولة تقديم برهان تقليدي على أن ناتج ضرب عددين سالبين هو عدد موجب. ويعتمد البرهان على افتراض أننا نرغب في أن يشمل نظامُ الأعدادِ الصحيحةِ المتوسعُ النظامَ الأصليَّ الخاصَّ بالأعداد الطبيعية، ويجب على النظام الأكبر مواصلة الخضوع لقواعد الجبر العادية. وبالفعل، تأتي نتيجة ذلك على ناتج ضرب عددين سالبين من أن أي عدد يُضرب في صفر يساوي صفرًا. (هذا أيضًا ليس افتراضًا، ولكنه بالأحرى نتيجة لقوانين الجبر.) لدينا الآن:

$$-1 \times (-1 + 1) = -1 \times 0 = 0;$$

إذا ضربنا الأقواس بعد ذلك، ندرك أنه لكي تُساوي الجهةُ اليسرى صفرًا، فإن الطرف $(-1) \times (-1)$ يجب أن يحمل العلامة المعكوسة للمعادلة $-1 = 1 \times (-1)$؛ بعبارة أخرى $1 = (-1) \times (-1)$.

## الكسور والأعداد النسبية

بالطريقة نفسها التي تؤدي بنا عمليةُ الطرح إلى الأعداد السالبة، تؤدي بنا أيضًا عمليةُ القسمة إلى الخروج من مجموعة أعداد العد الطبيعية إلى عالم الكسور الأكبر. مع ذلك، فطبيعة العملية الحسابية الجديدة التي نقابلها مختلفة. فعند الجمع أو الطرح، لا تتوافق الكسور ذات المقامات (العدد السفلي) المختلفة. وينبغي أن يُعبَّر عن الكسور محل النقاش باستخدام مقامٍ موحَّد قبل إتمام العملية الحسابية. أما الضرب، فهو عملية بسيطة نسبيًّا، كل ما نحتاجه فيها هو ضرب البَسْطَين (العددين العلويين) معًا والمقامين معًا من أجل الحصول على الإجابة. والقسمة هي العملية المعكوسة للضرب؛ لذا فالقسمة على $n$ توازي الضرب في مقلوبه $\frac{1}{n}$. وبوجه عام، ينتقل هذا الأمر إلى الكسور؛ إذ إنه للقسمة على الكسر $\frac{m}{n}$ نضرب في مقلوبه $\frac{n}{m}$؛ حيث إن ذلك يعكس تأثير الضرب في $\frac{m}{n}$.

كان المصريون القدماء راضين بـ «كسور الوحدة»، التي هي المقلوب البسيط للأعداد الصحيحة $\frac{1}{2}$، $\frac{1}{3}$، $\frac{1}{4}$، وما إلى ذلك (مع أنهم احتفظوا برمز خاص للكسر $\frac{2}{3}$). ولم يُنظر لكسر مثل $\frac{3}{4}$ كوحدة ذات معنًى في حد ذاته، وكانوا يسجلون هذه الكمية كناتج جمع مقلوبَين: $\frac{3}{4} = \frac{1}{2} + \frac{1}{4}$. (وترميز الكسور المستخدم هنا بالطبع من النوع الأوروبي

الحديث، الذي له أصول في الرياضيات الإغريقية.) مع ذلك، فليس من الواضح أنه من الممكن بالضرورة كتابة أيِّ كسرٍ كناتجِ جمعِ عددٍ من كسور الوحدة المختلفة، وهو ما أصروا عليه. مع ذلك، يمكن القيام بذلك دائمًا، وشرحُه سوف يسمح لك بصقل مهاراتك في التعامل مع الكسور.

إذا كنت ترغب في اكتشاف التحليل المصري لكسرٍ مثل $\frac{9}{20}$، فإن ما تحتاجه فحسب هو طرح أكبر كسر وحدة يمكنك طرحه من العدد المذكور، وتكرار هذه العملية، حتى يصبح الباقي نفسه كسر وحدة. سوف يأتي ذلك بثماره دائمًا، وعدد الكسور التي تنطوي عليها هذه العملية لا يتخطى أبدًا بسط الكسر الأصلي. هذا لأنه، في كل مرحلة، يظل بسط الكسر دائمًا أقل من البسط السابق؛ وذلك غير منطقي ولكنه حقيقي. في هذا المثال، سوف تحصل في المرحلة الأولى على:

$$\frac{9}{20} - \frac{1}{3} = \frac{27}{60} - \frac{20}{60} = \frac{7}{60};$$

بعد ذلك، نجد أن أكبر كسر وحدة أقل من $\frac{7}{60}$ هو $\frac{1}{9}$. (وللتأكد من ذلك، راجع نتائج الضرب التبادلي: $\frac{7}{60} < \frac{1}{9}$؛ لأن $9 \times 7 = 63 > 60 = 60 \times 1$.) وبالطرح مرة أخرى، نجد أن:

$$\frac{9}{20} - \frac{1}{3} - \frac{1}{9} = \frac{7}{60} - \frac{1}{9} = \frac{21}{180} - \frac{20}{180} = \frac{1}{180};$$

ومن ثم نستعيد التحليل المصري:

$$\frac{9}{20} = \frac{1}{3} + \frac{1}{9} + \frac{1}{180}.$$

إنَّ هذا النهجَ النَّهِم الذي يَطرح دائمًا أكبرَ كسْرِ وحدةٍ متاحٍ هو ناجح بالفعل، ولكن ربما لا يؤدي لأقصر عملية تحليل موجودة، كما نرى حتى في هذه الحالة؛ حيث إن $\frac{1}{5} + \frac{1}{4} = \frac{9}{20}$. مع ذلك، يمكن التوصل إلى عملية تحليل $\frac{9}{20}$ المكونة من كسرين من خلال استخدام الطريقة الموجودة في بردية أخميم، وهي مخطوطة إغريقية اكتُشفت في مدينة أخميم على النيل، ويعود تاريخها إلى ٥٠٠–٨٠٠ قبل الميلاد. وبالترميز الحديث، يمكن التعبير عن هذه الطريقة بالاتحاد الجبري الذي يسهل التحقق منه:

$$\frac{m}{pq} = \frac{m}{p(p+q)} + \frac{m}{q(p+q)}.$$

وبتطبيق هذه المعادلة عندما تكون $m = 9$، $p = 4$، $q = 5$، ينتج لنا على الفور $\frac{1}{5} + \frac{1}{4} = \frac{9}{5\times9} + \frac{9}{4\times9} = \frac{9}{20}$.

ربما مرت سنوات منذ آخر مرة جمعتَ فيها حتى كسور بسيطة معًا لأن كل العمليات الحسابية العملية تقريبًا تُجرى في الوقت الحالي باستخدام الصيغة العشرية. ولقد اكتُشف استخدام الكسور العشرية في الصين القديمة والأمم العربية في العصور الوسطى، ولكن لم ينتشر استخدامها في أوروبا إلا في الجزء الأخير من القرن السادس عشر، عندما بُذلَت جهود حثيثة من أجل تحسين الطرق العملية للحساب. مع ذلك، يوجد ثمن لا بد من دفعه مقابل الالتزام بالصيغة العشرية؛ ففي العمليات الحسابية في النظام العشري العادي، نستغل حقيقة أن أي عدد يمكن كتابته كمجموع مضاعفات قوى العشرة. وعندما نعبِّر عن كسر بصورة عشرية، فإننا نحاول كتابة العدد كمجموع قوى $0.1 = \frac{1}{10}$. ولكن للأسف، حتى بالنسبة للكسور البسيطة للغاية مثل $\frac{1}{3}$، لا يمكن القيام بذلك، ويستمر المفكوك (التمثيل) العشري بلا نهاية: $\frac{1}{3} = 0.333\ldots$. وفي الواقع، إننا ندرك أنه من خلال وقف تكرار المفكوك العشري بعد عدد معين من الخانات (اعتمادًا على الدقة التي نريدها)، يمكننا الحصول على الكسر العشري غير المتكرر الناتج، الذي يقترب من الكسر الصحيح. وأيُّ عدمِ دقةٍ يُعد هامشيًّا مقارنةً بالراحة الناجمة عن إجراء كل الأعمال الحسابية في الإطار المرجعي للنظام العشري المعياري. ويمكن النظر للمفكوك العشري على أنه أقرب ما يمكننا الحصول عليه للتوصل إلى مقام مشترك لكل الكسور.

مع ذلك، فمن الطبيعي أن نسأل: أيُّ كسر من الكسور سيتوقف تكرارُ مفكوكِه العشري (وأيها لن يتوقف تكرار مفكوكه)؟ الإجابة هي أنه ليس الكثير منها سيتوقف تكرار مفكوكه؛ ففي أكثر الأحيان، يتخذ المفكوك العشري للكسر نمطًا متكررًا: $\frac{3}{22} = 0.1363636\ldots$؛ حيث يتكرر جزء 36 للأبد. وكل كسر يولد كسرًا عشريًّا متكررًا بطريقة أو بأخرى، مع أنه في حالة الكسر العشري غير المتكرر مثل $\frac{1}{2} = 0.5$، فإن الجزء المتكرر يمثل ببساطة سلسلة لا متناهية من الأصفار: $\frac{1}{2} = 0.5000\ldots$؛ ولذلك لا تكتب صراحة. على أية حال، فإن طول الجزء المتكرر في أي مفكوك عشري متكرر لا يزيد عن قيمة أقل من قيمة المقام. يمكن إدراك ذلك بتأملِ ما يحدث عندما نُجري عملية القسمة المطولة المقابلة: فإذا كان المقام $n$، فإن الباقي بعد كل خطوة في القسمة سوف

يكون إحدى القيم $0, 1, \ldots, n - 1$. إذا كان الباقي في مرحلةٍ ما يساوي صفرًا، فإن القسمة تتوقف عن التكرار، وكذلك يتوقف تكرار المفكوك العشري: على سبيل المثال: $\frac{11}{40}$ يساوي بالضبط $0.275$. وإلا فإن القسمة تستمر للأبد، ولكن بمجرد أن يتكرر الباقي، وهو الأمر الذي لا مفر منه، سوف نُجبر على إجراء الحلقة نفسها من عمليات القسمة مرة أخرى، وهذا يقدم نمطًا متكررًا لن يَطول جزؤه عن $n - 1$. وسوف يتوقف تكرار المفكوك — بالضبط — عندما يكون المقام ناتجًا من نواتج العاملَين الأوليَّين 2 و5 من نظامنا العشري، ولكن لن يتوقف حال وجود عامل آخر. على سبيل المثال: الكسور ذات المقامات 16 و40 و50 كسور متناهية، ولكن كسور مثل $\frac{1}{14}$ و$\frac{1}{15}$ ليست متناهية ولن تتوقف عن التكرار؛ لأن العاملين الأوليَّين 7 و3 على الترتيب في مقاميهما يُجْبِران المفكوكَ على الدخول في دائرة متكررة.

مع ذلك، يبين هذا أن توقُّف مفكوك الكسر عن التكرار من عدمه لا يتحدد بالعدد نفسه فحسب، ولكن بالأحرى يعتمد على علاقة العدد بالقاعدة التي تعتمد عليها. فعلى سبيل المثال، إذا كنا نعمل وفق نظام ثلاثي (القاعدة ثلاثة)، فإن $0.1$ سوف تمثل $\frac{1}{3}$؛ حيث إن 1 بعد العلامة العشرية سوف يشير إلى $\frac{1}{3}$، وليس $\frac{1}{10}$، كما يشير في المفكوك العشري.

كذلك العملية المعاكسة بتحويل كسر عشري متكرر إلى كسر اعتيادي بسيطة للغاية، مما يدل على وجود تماثل ثنائي بين الكسور الاعتيادية والكسور العشرية المتكررة، ويمكننا استخدام أي تمثيل يتناسب بصورة أفضل مع غرضنا الحالي. ومثال بسيط على ذلك: افترض أن $a = 0.212121\ldots$. نظرًا لأن طول الجزء المتكرر عددان، فيمكننا تبسيط ذلك — كما سترى — من خلال الضرب في $10^2 = 100$ للحصول على $100a = 21.212121\ldots$. تم إعداد ذلك لكي تُلغي الأجزاءُ المتكررة للعددين $a$ و$100a$ — عند الطرح — بعضُها البعضَ لكونها متطابقة، فتسمح لنا باستنتاج أن $99a = 21$، وبذلك $a = \frac{21}{99} = \frac{7}{33}$.

وكثيرًا ما يُستخدم هذا النوع من الخدع لتبسيط أيِّ تعبير جبري ينطوي على عملية متكررة غير متناهية. على سبيل المثال، ألقِ نظرة على العبارة المركبة التالية:

$$a = \sqrt{2\sqrt{5\sqrt{2\sqrt{5}}}}\ldots$$

من خلال التربيع، ثم إعادة التربيع، يصبح الجانب الأيسر من المعادلة $a^4$، في حين يعطينا التعبير الجبري الذي على الجانب الأيمن:

$$a^4 = 2^2 \times 5 \times \sqrt{2\sqrt{5\sqrt{2\sqrt{5}}}}\ldots$$

نظرًا لأن ما يتلو 5 هو نسخة أخرى من التعبير الجبري الممثل لـ $a$، نستنتج أن $a^4 = 20a$ بحيث $a^3 = 20$ أو، إذا كنت تفضل، $a$ هو الجذر التكعيبي لـ 20. سوف نعود لهذه الطريقة مجددًا في الفصل السابع عندما نتناول ما يطلق عليه الكسور المستمرة.

هل تقدم لنا فئة الكسور كل الأعداد التي قد نحتاجها؟ كما ذكر آنفًا، مجموعة الكسور جميعها — مع الكسور السالبة المقابلة لها — تكوِّن مجموعة الأعداد المعروفة باسم الأعداد النسبية، وهي كل الأعداد الناتجة عن الأعداد الصحيحة والنسب بينها. وهي ملائمة لإجراء العمليات الحسابية؛ إذ إن أي ناتج ينتج عن العمليات الحسابية الأربع الأساسية — الجمع والطرح والقسمة والضرب — لن يأخذك بعيدًا عن عالم الأعداد النسبية. وإذا كنا سعداء بذلك، فإن مجموعة الأعداد تلك هي كل ما نحتاجه. مع ذلك، سنوضح في الجزء التالي كيف تكون الأعداد على غرار $a$ السابق غير نسبية.

## الأعداد غير النسبية

تعني الصفة «غير نسبي» ببساطة — عندما تنطبق على العدد $a$ — أن العدد ليس نسبيًّا؛ أي إنه لا يمكن كتابته في صورة كسر. ولقد اكتُشفت الأعداد غير النسبية لأول مرة منذ فترة طويلة في عصر الإغريق. فَهِمَ فيثاغورس الطبيعة غير النسبية للجذر $\sqrt{2}$. ولم يفكر الإغريق من منظور المفكوك العشري، ولكنهم كانوا راضين بمعرفة الطول الموضح في هندسة المسطرة والفرجار بأنه يمثل قيمة حقيقية. وبوجه خاص، تنص نظرية فيثاغورس على أن الضلع الأطول في مثلث قائم الزاوية — الذي يبلغ طول ضلعيه القصيرين وحدة واحدة — يساوي بالضبط الجذر التربيعي للعدد 2.

كان فيثاغورس قادرًا على إثبات أن الجذر التربيعي للعدد 2 لا يساوي أي كسر؛ ومن ثَم أوضح أن الأعداد غير النسبية موجودة حقًّا. على وجه الخصوص، لا يمكنك قياس قطر مربع على نحو دقيق بالوحدات نفسها التي تقيس بها الضلع؛ لأنه إذا كنت

تستطيع، فإن القطر سيكون — بالضبط — مضاعف كسري للضلع، وفي هذه الحالة سيكون $\sqrt{2}$ مساويًا لهذا الكسر. مع ذلك، يتعارض الطولان تعارضًا جذريًّا، أو فلنقُلْ «لا يمكن قياسهما» بالطريقة المذكورة في النصوص القديمة. وينطبق الأمر نفسه على $\pi$، التي تساوي تقريبًا الكسر $\frac{22}{7}$، ولكنها مختلفة عنه وعن أي كسر ترغب في ترشيحه لها. (مع ذلك، فالنسبة سهلة التذكر المكونة من «زوج من 1، وزوج من 3، وزوج من $5'$»: $355/113 = 3.1415929\ldots$ تقترب بدقة من قيمة $\pi$ لأكثر من جزء من المليون.)

مع أنه من الصعوبة بمكان إثبات أن $\pi$ غير نسبية، فإنه يمكن تسوية مشكلة الجذر التربيعي للعدد 2 بسهولة من خلال برهان تناقُض بسيط. أولًا، نلاحظ أنه بالنسبة لأي عدد $c$، فإن أعلى قوة للعدد 2 التي هي عامل للعدد $c^2$، تُعد ضعف أعلى قوة للعدد 2 التي هي عامل للعدد $c$. ومن ثم فإن أعلى قوة للعدد 2 — على نحو خاص — تقسِّم أي عدد مربع، يجب أن تكون في حد ذاتها عددًا زوجيًّا. على سبيل المثال، $24 = 2^3 \times 3$، بينما $576 = 24^2 = 2^6 \times 3^2$، وفي هذه الحالة أعلى قوة للعدد 2، تقسم العدد، تتضاعف بالفعل من 3 إلى 6 عند التربيع. وهذه هي الحال دائمًا، ولا تنطبق بالفعل على قوى 2 فحسب، ولكن تنطبق أيضًا على أي عامل أوَّلي للعدد الأصلي.

افترض الآن أن $\sqrt{2}$ كان يساوي الكسر $\frac{a}{b}$. فبتربيع كلا طرفي هذه المعادلة، يمكننا استنتاج أن $\frac{a^2}{b^2} = 2$، وهو ما يؤدي إلى $2b^2 = a^2$. ومن خلال الملاحظة السابقة نرى أن أعلى قوة للعدد 2 — تقسم الطرف الأيمن من هذه المعادلة — زوجية، في حين أن أعلى قوة تقسم الطرف الأيسر فردية (بسبب وجود 2 الإضافية). وهذا يبين أن المعادلة لا قيمة لها؛ ومن ثم يجب ألَّا يكون ممكنًا كتابة $\sqrt{2}$ في صورة كسر في المقام الأول. ومثل فيثاغورس، نواجه نحن أيضًا الأعداد غير النسبية.

البراهين من هذا النوع تسمح لنا بإيضاح أنه بوجه عام إلى حدٍّ ما، عندما نأخذ الجذر التربيعي (أو التكعيبي أو أي جذر أكبر) لعدد ما، فإن الناتج — إذا لم يكن عددًا صحيحًا — دائمًا ما يكون عددًا غير نسبي، وهذا يفسر السبب في أن الكسر العشري على شاشة آلتك الحاسبة لا يُظهر أبدًا نمطًا متكررًا عند ضرورة حساب هذا الجذر.

اكتشف فيثاغورس أنه لكي يجري حساباته، فإن ذلك يتطلب مجالًا من الأعداد أوسع من مجرد الكسور. وكان الإغريق يعتبرون العدد حقيقيًّا إذا كان طوله يمكن تكوينه باستخدام فاصل وحدة معيارية باستعمال مسطرة (ليست مسطرة مخططة، مجرد حافة فحسب) وفرجار. واتضح أنه على الرغم من أن عمليات الجذر التربيعي

تنتج بالفعل أعدادًا غير نسبية، فإن المجموعة بأكملها لا تتخطى كثيرًا الأعداد النسبية. فالأعداد الإقليدية — كما سنشير إليها — هي كل هذه الأعداد التي يمكن التوصل إليها من العدد $1$ من خلال إجراء أيٍّ من العمليات الحسابية الأربع أو جميعها، وأخْذ الجذور التربيعية لأي عدد من المرات. على سبيل المثال، العدد $\sqrt{7 - \sqrt{4/3}}$ هو عدد من هذا النوع. وحتى الجذور التكعيبية تتخطى حيز الأدوات الإقليدية. وكان ذلك أساس أول مسألة كبيرة غير محلولة في الرياضيات على الأرجح. وكانت أول مسألة من مسائل ديليان الثلاث — كما كان يطلق عليها — عبارة عن طلب التوصل للجذر التكعيبي للعدد $2$، باستخدام مسطرة وفرجار فحسب. وتقول الأسطورة إن هذه كانت المهمة التي وضعها الرب عندما استشار مواطنو جزيرة ديلوس عرَّافةَ دلفي من أجل معرفة ما ينبغي عليهم فعله من أجل إبعاد الطاعون عن أثينا؛ فصيغتِ المسألة في صورة مضاعفة حجم المذبح بالضبط، الذي كان عددًا مكعبًا مثاليًّا.

فظلت هذه المسألة بلا حل في العصور القديمة؛ ولم يُتوصل إلى أن الجذر التكعيبي للعدد $2$ كان يتجاوز قدرة الأدوات الإقليدية إلا في عام ١٨٣٧ على يد بيير وانتسل (١٨١٤–١٨٣٨)؛ حيث كان الأمر يتطلب وصفًا جبريًّا دقيقًا لما هو ممكن باستخدام الأدوات الكلاسيكية من أجل إدراك أن الجذر التكعيبي للعدد $2$ هو عدد من نوع مختلف جوهريًّا. وتَعَلَّق الحل بإيضاح أنه لا يمكن أبدًا استخراج جذور تكعيبية من الجذور التربيعية والأعداد النسبية. وعند صياغة الأمر بهذه الطريقة، تبدو الاستحالةُ معقولةً على نحو أكبر، مع أن هذا لا يمثِّل برهانًا على الإطلاق.

### الأعداد المتسامية

تقع عائلة الأعداد المتسامية الغامضة ضمن مجموعة الأعداد غير النسبية؛ وهذه الأعداد لا تظهر من خلال الحسابات العادية للعمليات الحسابية واستخراج الجذور. ومن أجل التعريف الدقيق، نقدم أولًا مجموعة الأعداد الجبرية المتممة، وهي الأعداد التي تَحل بعض المعادلات متعددة الحدود التي تتضمن معاملات صحيحة: على سبيل المثال، المعادلة $x^5 - 3x + 1 = 0$ مثال على هذه المعادلات. ومن ثم يشار إلى الأعداد المتسامية بأنها مجموعة الأعداد غير الجبرية.

ليس من الواضح على الإطلاق أن مثل هذه الأعداد موجودة بالفعل. مع ذلك، فهي موجودة بالفعل وتكوِّن مجموعة سرية للغاية، لا يفشي أعضاؤها سرَّ انتسابهم لها

بسهولة. على سبيل المثال، العدد $\pi$ مثال على العدد المتسامي، ولكن هذه ليست حقيقة تنكشف علنًا. وسوف نوضح في الفصل التالي على نحو دقيق — عند استكشاف طبيعة المجموعات غير المنتهية — لماذا تُعد «معظم» الأعداد أعدادًا متسامية.

في الوقت الحاليِّ، سوف أكتفي بتقديم ما ربما يكون أشهر الأعداد المتسامية على الإطلاق، وهو العدد $e = 2.71828\ldots$. يظهر هذا العدد باستمرار في الرياضيات المتقدمة والتفاضل والتكامل. إنه أساس ما يطلق عليه اللوغاريتم الطبيعي، الدالة التي تخبرك بالمساحة الواقعة وراء الرسم البياني لدالة المقلوب. وهو أيضًا القيمة النهائية لمتتالية الأعداد التي تحصل عليها عند رفع نسبة عددين صحيحين متتاليين — $\frac{n+1}{n}(= 1 + \frac{1}{n})$ — للقوة $n$. (استخدم آلتك الحاسبة لحساب قيمة $(129/128)^{128}$؛ ويمكنك تسريع عملية رفع الأس تلك: احسب فحسب $129/128$ ثم قم بتربيع الناتج سبع مرات؛ إذ إن $2^7 = 128$.)

تظهر هذه المتتالية عندما نفكر في مسألة القيمة النهائية لمعدل فائدة مركبة، في حين تقلل الفواصل الزمنية للسداد على نحو أقصر من فاصل سنويٍّ إلى شهريٍّ إلى يوميٍّ، وما إلى ذلك. ولتوضيح هذه الفكرة بأفضل صورة، افترضْ أن الفائدة تُدفع بمعدل سنوي $100$ بالمائة، مضاعفًا قسط $n$ في السنة؛ مما يعني أن استثمارك الأولي يُضرب في عامل $(1 + \frac{1}{n})$، بعدد مرات $n$ في كل شهر على مدار العام. حينها سيضرب رأس مالك في العامل $(1 + \frac{1}{n})^n$. وكلما زاد عدد مرات دفع الفائدة كسبْتَ أكثر؛ حيث تبدأ في جمع فائدة على فائدتك في وقت أسبق؛ لأن $n$ تصبح أعلى. مع ذلك، في حين تزداد قيمة $n$، فإن معدل النسبة المئوية السنوي الفعَّال لا يزيد ليتجاوز كل الحدود، ولكنه بالأحرى يصل إلى السقف، أو كما يطلق عليه علماء الرياضيات: إلى النهاية العليا. والمضروب فيه المحدِّد هذا — الذي ينطبق على رأس مالك في حالة الفائدة المستمرة، في حين $n$ تزداد — هو القيمة النهائية للعدد:

$$\left(1 + \frac{1}{n}\right)^n \longrightarrow e = 2.71828\ldots$$

توجد طريقة أخرى يظهر من خلالها العدد $e$ الغامض من خلال مجموع مقلوب المضروب، وهذه الطريقة توفر وسيلة لحساب $e$ بدرجة دقة عالية؛ حيث تتجمع هذه السلسلة بسرعة لأن حدودها تصل إلى الصفر سريعًا في الواقع:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \cdots$$

يسمح لك هذا التمثيل بأن تبيِّن من خلالِ برهانِ تناقضٍ بسيطٍ نسبيًّا — مذكور هنا — أن $e$ عدد غير نسبي. نفترض أن المتتالية السابقة للعدد $e$ تساوي الكسر $\frac{p}{q}$ ثم نضرب كِلا الطرفين في $q!$. الطرف الأيسر حينها سيكون عددًا صحيحًا، ولكن الطرف الأيمن سيتكون من حدود من أعداد صحيحة متبوعة بسلسلة لا متناهية من حدود غير صحيحة. ومن خلال المقارنة بمتتالية هندسية بسيطة، نستنتج أن هذا «الذيل» يؤدي إلى أقل من 1؛ ومن ثم لا يمكن أن يكون الطرف الأيمن عددًا صحيحًا، وهنا يكمن التناقض المطلوب. وإيضاح أن $e$ ليس عددًا غير نسبي فحسب، بل عدد متسامٍ أيضًا، يتطلب المزيد من الجهد.

علاقة $e$ مع المضروب تُظهر نفسها أيضًا في معادلة شهيرة لعالم الرياضيات الاسكتلندي جيمس سترلينج (١٦٩٢–١٧٧٠)، الذي سميت أعداد سترلينج (انظر الفصل الخامس) تيمُّنًا به. أوضح سترلينج أنه كلما زادت $n$، تُقرب قيمة $n!$ أفضل وأفضل بالتعبير الجبري $\sqrt{2\pi n}\left(\frac{n}{e}\right)^n$.

نظرًا لأن $e$ تَظهر بطرق متنوعة مختلفة وبسيطة إلى حدٍّ ما، فإنها تظهر باستمرار في جميع فروع الرياضيات، وغالبًا حيث لا تتوقع أن تجدها. على سبيل المثال، خذ مجموعتين من أوراق اللعب — مخلوطتين بغير نظام — واقلب الورقة العلوية لكل مجموعة، وقارن بينهما. استمر في فعل ذلك حتى تنتهي من قلب أوراق المجموعتين كلتيهما. ما احتمالات أنه في مرحلةٍ ما سوف تصل لتطابُق تام؟ أي إنه في إحدى المرات تكون الورقتان الظاهرتان هما نفس الورقة بالضبط؛ مثلًا ورقتا السبعة من نوع الأسباتي أو القلوب أو أي نوع. يُستنبط من هذا أن نسبة المرات التي تؤدي فيها هذه التجربة إلى تطابُق واحد من هذا النوع على الأقل توشك ألا تختلف عن $\frac{1}{e}$، التي تصل إلى حوالي 36.8 بالمائة. وينتج هذا من تطبيق ما يعرف بـ «مبدأ التضمين والاستبعاد»، الذي يصل إلى الحل عن طريق مجموع حدود، يمثل كلٌّ منها تصحيحاتٍ متبادلة أو تصحيحات متعاكسة. وفي هذا المثال، يقدم المبدأ — هذه المرة — سلسلة مقلوبات المضروبات مع إشارات متبادلة تتقارب إلى $\frac{1}{e}$.

## الأعداد الحقيقية والأعداد التخيلية

تعاملت الفصول الخمسة الأولى من هذا الكتاب — على نحو رئيسي — مع الأعداد الصحيحة الموجبة. وركزنا على سماتِ عمليةِ تحليلِ هذه الأعداد الصحيحة إلى عوامل،

وهو ما قادنا إلى التعرف على أعداد لا تخضع بطريقة سليمة لعملية التحويل إلى عوامل؛ وهي الأعداد الأولية؛ المجموعة التي تحتل موقعًا محوريًّا في التشفير الحديث. وكذلك دَرَسْنا أنواعًا معينة من الأعداد مثل أعداد ميرسين الأولية، التي ترتبط ارتباطًا وثيقًا بالأعداد الكاملة، وقضينا وقتًا في تقديم بعض الفئات الخاصة من الأعداد الصحيحة التي تُعد مهمة في حساب مجموعات معينة تنشأ على نحو طبيعي. وكانت خلفية ذلك كله نظام الأعداد الصحيحة، وهي أعداد العد الموجبة والسالبة والصفر.

تجاوزنا في هذا الفصل الأعداد الصحيحة، أولًا إلى الأعداد النسبية (الكسور، سواء كانت موجبة أو غير ذلك)، ثم إلى الأعداد غير النسبية، وضمن فئة الأعداد غير النسبية تَعرَّفنا على الأعداد المتسامية. والنظام الأساسي الذي تقع ضمنه كل هذه الأعداد هو نظام الأعداد الحقيقية، الذي يمكن التفكير فيه بوصفه مجموعة كل المفكوكات العشرية الممكنة. ويمكن تمثيل أي عدد حقيقي موجب بالصيغة $r = n \cdot a_1a_2 \ldots$؛ حيث يكون $n$ عددًا صحيحًا غير سالب، وتُتبع العلامة العشرية بسلسلة لا متناهية من الأرقام. وإذا وصلت هذه السلسلة في النهاية إلى نمط متكرر، فإن $r$ يكون في الواقع عددًا نسبيًّا، وقد أوضحنا كيفية تحويل هذا التمثيل إلى كسر اعتيادي. وإذا لم تصل لنمط متكرر، فإن $r$ يكون عددًا غير نسبي؛ ومن ثم فإن الأعداد الحقيقية تنقسم لهاتين المجموعتين: أعداد نسبية وأعداد غير نسبية.

في تخيلاتنا الرياضية، غالبًا ما نتصور الأعداد الحقيقية على أنها تقابل كل النقاط الموجودة على خط الأعداد، في حين ننظر من الصفر نحو اليمين من أجل رؤية الأعداد الحقيقية الموجبة، ثم نحو اليسار من أجل رؤية الأعداد الحقيقية السالبة. وهذا يخلف لنا صورة متماثلة؛ حيث تمثِّل الأعداد الحقيقية السالبة صورة معكوسة للأعداد الحقيقية الموجبة، ويُحافظ على هذا التماثل عند التعامل مع الجمع والطرح؛ ولكن ليس عند التعامل مع الضرب. فبمجرد الانتقال إلى الضرب، تختفي الحالة المتساوية بين الأعداد السالبة والموجبة؛ مثل العدد 1 الذي يمتلك خاصية لا يمتلكها أي عدد آخر؛ إذ إنه «المحايد الضربي»؛ بمعنى أن $1 \times r = r \times 1 = r$، لأي عدد حقيقي $r$. إن الضرب في 1 يثبِّت موقع أي عدد، ولكن — في المقابل — الضرب في $-1$ ينقل العدد إلى صورته المعكوسة على الجانب الآخر من الصفر. وبمجرد دخول الضرب للمشهد، فإن الاختلافات الجوهرية لطبيعة الأعداد الموجبة والسالبة تظهر. وعلى وجه الخصوص، تفتقد الأعداد السالبة الجذور التربيعية داخل نظام الأعداد الحقيقية؛ لأن مربع أي عدد حقيقي دائمًا ما يكون أكبر من الصفر أو مساويًا له.

وهذه هي إشارة وصول الأعداد التخيلية. ولسوف نتناول هذا الموضوع مرة أخرى في الفصل الأخير؛ وسوف نقدم بعض التعليقات التمهيدية حوله في الوقت الراهن.

تظهر هذه الأعداد عند البحث عن حلول للمعادلات البسيطة متعددة الحدود. فعلى نحو خاص، نظرًا لأن مربع أي عدد حقيقي لا يكون سالبًا أبدًا، فلا يمكننا إيجاد حل للمعادلة $x^2 = -1$. وبشجاعة، اخترع علماء الرياضيات حلًّا يشار إليه $i$، وهو يمتلك تلك الخاصية؛ لذا فإن $i^2 = -1$. للوهلة الأولى، يبدو هذا مصطنعًا واعتباطيًّا ولكنه لا يختلف كثيرًا عن السلوك الذي انخرطنا فيه من قبل. فبالرغم من كل شيء، في حين ندرك أن أعداد العد 1، 2، 3 ... أهم من غيرها، فإننا — لكي نتعامل بسلاسة مع الأمور العامة للأعداد — نتوجه إلى نظام الأعداد النسبية الأوسع نطاقًا، الذي يجمع كل الكسور والأعداد الموجبة والسالبة والصفر. مع ذلك، اكتشفنا بعدها أننا ليس لدينا حل للمعادلة $x^2 = 2$؛ إذ إننا أوضحنا أن مربع أي عدد نسبي لا يمكن أن يساوي 2 بالضبط. وللتعامل مع ذلك، كان علينا اختراع $\sqrt{2}$. وعند هذه النقطة، أمكننا أن نسلك التوجه البديل، ونقول إننا أثبتنا أن الجذر التربيعي للعدد 2 ببساطة غير موجود، وتلك هي نهاية الأمر. مع ذلك، فقليلٌ مَن يشعرون بالرضا لإغلاق هذا الباب بهذه الطريقة. فبالتأكيد، لم يكن الإغريق راضين بترك الأمر عند هذه النقطة؛ إذ كان بإمكانهم تكوين مفكوك يمثل $\sqrt{2}$ باستخدام الفرجار والمسطرة؛ ومن ثم كان العدد — وفق طريقة تفكيرهم — حقيقيًّا تمامًا، وأيٌّ من الأنظمة الرياضية كان ينكر ذلك اعتُبر منقوصًا.

ربما نتفق مع فيثاغورس لسبب مختلف تمامًا. ربما نَرُدُّ بقول إننا يمكننا تقريب $\sqrt{2}$ إلى أي درجة من الدقة من خلال مفكوكه العشري: $\sqrt{2} = 1.414213\ldots$، وبهذا فإن $\sqrt{2}$ يكون العدد الذي يُمثل — بدقة — بإجمالي مفكوكه. وربما يجد المرء في العصور الحديثة مزيدًا من القوة في هذا البرهان، ويُصِر لهذا السبب على أن نظام الأعداد يحتاج للمفكوك إلى ما وراء الأعداد النسبية.

مع ذلك، ربما نقول من الوهلة الأولى إن الأمور مختلفة عندما تتعلق بالعدد $\sqrt{-1}$؛ إذ إنه لا يبدو أن هناك حاجة مُلِحَّة للقلق حِيالَ عدم ظهوره بين مجموعة الأعداد التي نطلق عليها في العادة أعدادًا حقيقية. ويتضح من ذلك أنه بينما يتقدم علم الرياضيات لدينا لأبعد من ذلك قليلًا، فإن الحاجة لوجود أعداد تخيلية تصبح مُلحَّة للغاية، وأي ممانعة أولية للتعامل معها تتبدد عندما يزداد فهمنا للأمور الرياضية.

ظهر أول عدد من هذا النوع في القرن السادس عشر، عندما تعلَّم علماءُ رياضيات إيطاليون كيفيةَ حل المعادلات متعددة الحدود التكعيبية ومن الدرجة الرابعة بطريقةٍ

تُوسِّع نطاق الطريقة المستخدمة في حل المعادلات التربيعية. غالبًا ما تتضمن طريقة كاردانو — كما أطلق عليها — جذورًا تربيعية للأعداد السالبة، مع أنه قد تَبيَّن في النهاية أن حلول المعادلات أعداد صحيحة موجبة. ومن خلال مراحل بدأت بهذه النقطة تم توضيح أن استخدام الأعداد المركبة — التي تأخذ الصيغة $a + bi$؛ حيث $a$ و$b$ عددان حقيقيان عاديان — يُسهل إجراء مجموعة متنوعة من الحسابات الرياضية. على سبيل المثال، كشف أويلر في القرن الثامن عشر المعادلة الصغيرة المدهشة $e^{i\pi} = -1$ واستغلها، وهي لا تخفق أبدًا في إدهاشِ أيٍّ شخص يقابلها لأول مرة.

وفي بدايات القرن التاسع عشر تقريبًا، درس وِسِل وأرجاند التفسير الهندسي للأعداد المركبة بوصفها نقاطًا على المستوى الإحداثي (النظام المعياري للإحداثيين $y$ و$x$)، ومنذ ذلك الحين أصبح استخدام الأعداد «التخيلية» مقبولًا بوصفه رياضيات عادية. ويسمح تحديد العدد المركب $x + iy$ بنقطة على المحورين $(x, y)$ بدراسة سلوك الأعداد المركبة من ناحية سلوك النقاط على المستوى الإحداثي، واتضح أن ذلك يساعد كثيرًا في الفهم. إن نظرية «المتغيرات المركبة» — التي يُمثِّل موضوعها بدوالِّ الأعداد المركبة، وليس الأعداد الحقيقية فحسب — ازدهرت على نحو مذهل على يدي أوجستين كوشي (١٧٨٩–١٨٥٧). وهي الآن ركيزة من ركائز الرياضيات، وتشكِّل أساسَ قدرٍ كبيرٍ من نظرية الإشارة الكهربية، كما يعتمد مجال حيود الأشعة السينية بأكمله على الأعداد المركبة. وثَبَتَ أن هذه الأعداد لها معنًى حقيقي، وأدهى من ذلك أن النظام مكتمل؛ حيث إن كل معادلة متعددة الحدود لها مجموعتها الكاملة من الحلول داخل منظومة الأعداد المركبة. وسوف نعود إلى هذا الموضوع في الفصل الأخير. ولكن قبل أن نفعل ذلك، سوف نتناول الطبيعة غير المتناهية لخط الأعداد الحقيقية بالتفصيل في الفصل التالي.

الفصل السابع

# نحو عدم التناهي وما بعده!

## لا تناهي في عدم التناهي

كان العالم الإيطالي الموسوعي العظيم جاليليو جاليلي الذي عاش في القرن السادس عشر (١٥٦٤–١٦٤٢) هو أول من نَبَّهَنَا إلى حقيقة أن طبيعة المجموعات غير المتناهية تختلف جذريًّا عن المجموعات المتناهية. وكما ذُكر في بداية هذا الكتاب، يكون حجم المجموعة «المتناهية» أصغر من حجم مجموعة ثانية، إذا أمكن إقران أفراد المجموعة الأولى مع أفراد يمثِّلون جزءًا وحسب من المجموعة الثانية. مع ذلك، يمكن على النقيض جعل المجموعات غير المتناهية تتطابق بهذه الطريقة مع مجموعات فرعية منها نفسها (حيث أعني بمصطلح «مجموعة فرعية» مجموعةً ضِمن المجموعة نفسها). وليس علينا الذهاب إلى ما هو أبعد من سلسلة أعداد العد الطبيعية 1، 2، 3، 4 ... لكي نشهد ذلك. فمن السهل وصف أي عدد من المجموعات الفرعية لهذه المجموعة التي تُشكل بنفسها قائمة لا متناهية، والتي تكون في تطابق ثنائي مع المجموعة كلها (انظر شكل ٧-١): الأعداد الفردية 1، 3، 5، 7 ... والأعداد المربعة 1، 4، 9، 16 ... والأعداد الأولية 2، 3، 5، 7 ... (على نحو أقل وضوحًا) وفي كل حالة من هذه الحالات، فإن المجموعات المتممة لها على الترتيب — الأعداد الزوجية والأعداد غير المربعة والأعداد المركبة — مجموعات لا متناهية أيضًا.

## فندق هيلبرت

هذا فندق غير عاديٍّ، دائمًا ما يرتبط بديفيد هيلبرت (١٨٦٢–١٩٤٣)؛ عالم الرياضيات الألماني الرائد في عصره الذي عمل على تمثيل الطبيعة الغريبة للامتناهي. السمة الرئيسية

في الفندق هي أنه يحتوي على عدد لا متناهٍ من الغرف، مرقمة 1، 2، 3 ... ولذا يتباهى دائمًا بوجود غرف شاغرة فيه.

| 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | |
|---|---|---|---|---|---|---|---|---|---|---|
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ◦ ◦ ◦ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | |
| ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ↕ | ◦ ◦ ◦ |
| 1 | 4 | 9 | 16 | 25 | 36 | 49 | 64 | 81 | 100 | |

شكل ٧-١: الأعداد الزوجية والأعداد المربعة مقرونة مع الأعداد الطبيعية.

مع ذلك، في إحدى الليالي كان الفندق ممتلئًا في الواقع — بمعنى أن كل غرفة بها ضيف — وما تسبَّب في حيرةِ موظف الاستقبال أن زبونًا إضافيًّا جاء طالبًا غرفة. تدخَّل المدير تجنبًا لأي موقف سيئ، وأخذ الموظف جانبًا ليشرح له كيفية التعامل مع هذا الموقف، قائلًا له: أخبِر نزيل الغرفة 1 بالانتقال للغرفة 2، ونزيل الغرفة 2 بالانتقال للغرفة 3، وهكذا؛ بمعنى أننا نُصدر طلبًا عامًّا بأن النزيل الساكن في غرفة $n$ ينبغي أن ينتقل للغرفة $n + 1$، وهذا سيخلي الغرفة 1 لهذا السيد!

وهكذا، كما ترى، يوجد دائمًا غرف شاغرة في فندق هيلبرت. ولكن كم غرفة؟

في مساء اليوم التالي، واجه الموظف موقفًا مشابهًا لكنه أكثر تحديًا؛ إذ وصلتْ هذه المرة سفينةُ فضاء تحمِل 1729 راكبًا، وكلٌّ منهم طلب غرفة في الفندق المأهول بأكمله. مع ذلك، تعلَّمَ الموظفُ الدرسَ من الليلة الماضية وأدرك كيفية توسيع نطاق الفكرة للتعامل مع هذه المجموعة الإضافية من النزلاء. فأَخبَر النزيل المقيم في غرفة رقم 1 بالانتقال إلى غرفة رقم 1730، والمقيم في غرفة 2 بالانتقال إلى الغرفة 1731، وهكذا، يُصدر طلبًا عامًّا بأنه ينبغي على النزيل الذي يسكن في الغرفة $n$ الانتقال إلى الغرفة $n + 1729$. وهذا يجعل الغرف من 1 حتى 1729 شاغرة من أجل القادمين الجدد، ويحق لموظفنا أن يشعر بالفخر بنفسه؛ لأنه تعامل مع هذا الشكل الجديد من مشكلة أمس بنفسه.

مع ذلك، ففي الليلة الأخيرة واجه الموظف مرة أخرى الموقف نفسه؛ فندق ممتلئ، ولكن هذه المرة — ما أصابه بالرعب — لم يأتِ بضعة نزلاء إضافيين فقط، ولكن حافلة فضائية لا متناهية تحمل عددًا لا متناهيًا من الركاب، كلٌّ منهم يقابِل أحد أعداد العد 1، 2، 3 ... قال الموظف الذي عانى وطأة هذه المشكلة لسائق الحافلة: إن الفندق ممتلئ ولا يوجد طريقة يمكنه تخيُّلها للتعامل معهم جميعًا. ربما يكون قادرًا على إقحام واحد أو اثنين إضافيين، أو ربما أي عدد محدود منهم، ولكن بالتأكيد ليس المزيد من الضيوف غير المتناهين. إنه لَأمر مستحيل بكل وضوح!

كانت ستحدث بَلبلة لا متناهية لولا تدخُّل المدير تارة أخرى في الوقت المناسب؛ حيث كان ملمًّا بدروس جاليليو حول المجموعات غير المتناهية، فأَعْلَمَ سائقَ الحافلة أنه لا توجد مشكلة على الإطلاق؛ إذ إنه توجد غرف شاغرة دائمًا في فندق هيلبرت لأي شخص. وأخذ موظفه المذعور جانبًا لتلقينه درسًا آخر؛ قال له: إن كلَّ ما علينا فعله هو الآتي: نخبر النزيل في غرفة 1 بالانتقال إلى غرفة 2، والنزيل في غرفة 2 بالانتقال إلى غرفة 4 والنزيل في غرفة 3 بالانتقال إلى الغرفة 6 وهكذا. وبوجه عام، ستكون التعليمات العامة هي أن النزيل في الغرفة $n$ ينبغي أن ينتقل للغرفة $2n$. وهذا سيجعل الغرف ذات الرقم الفردي شاغرة من أجل المسافرين على متن حافلة الفضاء غير المتناهية. لا مشكلة في ذلك على الإطلاق!

يبدو أن المدير يُحكم سيطرته على كل شيء. مع ذلك، حتى هو ربما يقع في مشكلة إذا اتضح أن سفينة فضاء تمتلك — بطريقةٍ ما — تقنيةً لِحَمْل راكب لكلِّ نقطة على طول خط الأعداد الحقيقية. فشخصٌ لكل عدد عشري سوف يتجاوز سعة فندق هيلبرت، وسوف نعرف السبب في ذلك في الجزء التالي.

## مقارنات كانتور

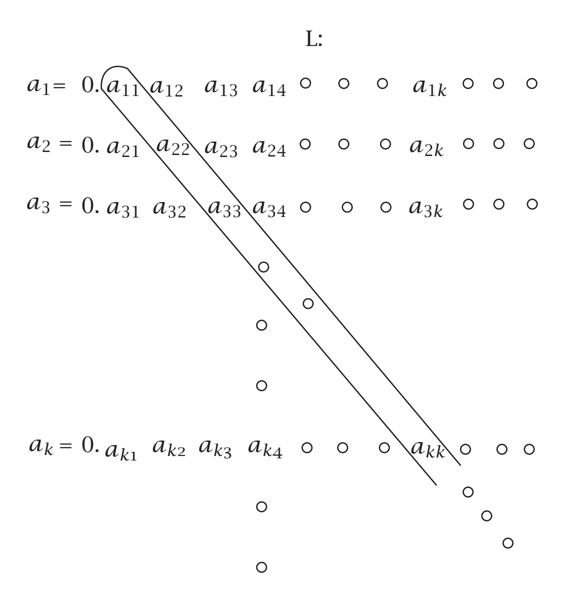
ربما يبدو كل هذا مستغرَبًا عندما تفكِّر به لأول مرة، ولكنْ ليس من الصعب تقبُّل أنَّ سلوك هذه المجموعات غيرِ المتناهية قد يختلف في بعض النواحي عن المجموعات المتناهية، وأنَّ خاصية امتلاك حجمٍ يساوي حجمَ إحدى مجموعاتها الفرعية هي مثالٌ على ذلك. مع ذلك، ففي القرن التاسع عشر، تَعمَّق جورج كانتور (١٨٤٥–١٩١٨) أكثر، واكتشف أنه لا يمكن اعتبار أن كل المجموعات غير المتناهية تمتلك عددًا كبيرًا متساويًا

من الأفراد. ولم يكن هذا الاكتشاف متوقَّعًا بطبيعته، ولكن ليس من الصعب إدراكه بمجرد لَفْتِ انتباهك له.

يطلب كانتور منا أن نفكر فيما يلي: افترِض أن لدينا أي قائمة لا متناهية $L$ مكونة من الأعداد $a_1, a_2, \ldots$ المقدمة في صورة عشرية؛ إذن، من الممكن كتابة أي عدد $a$ لا يظهر في أي مكان في القائمة $L$: ببساطةٍ نفترض أن $a$ مختلف عن $a_1$ في المنزلة العشرية الأولى بعد العلامة العشرية، ومختلف عن $a_2$ في المنزلة العشرية الثانية، ومختلف عن $a_3$ في المنزلة العشرية الثالثة، وهكذا؛ وبهذه الطريقة ربما يمكننا تكوين عددنا $a$، مع التأكد من أنه لا يساوي أي عدد في القائمة. هذه الملاحظة لا يمكن الاعتراض عليها، ولكن لها نتيجة مباشرة؛ هي أنه من المستحيل تمامًا للقائمة $L$ أن تتضمن كل الأعداد؛ لأن العدد $a$ سيكون ناقصًا من القائمة $L$. ويتبع ذلك أن مجموعة الأعداد الحقيقية كلها — التي هي عبارة عن أعداد مكونة من مفكوكات عشرية — لا يمكن كتابتها في قائمة، أو بعبارة أخرى، لا يمكن وضعها في تماثُل ثنائي مع أعداد العد الطبيعية، بالطريقة التي رأيناها في شكل ٧-١. وهذا الاستنتاج يُعرف باسم «برهان كانتور القطري»؛ حيث إن العدد $a$ الذي يقع خارج المجموعة $L$ يتشكل من خلال تخيُّل قائمة من التمثيلات العشرية للمجموعة $L$، كما هو مذكور في الشكل ٧-٢، وتحديد $a$ من خلال قطر المصفوفة.

وهنا يمكن القيام ببعض الخداع؛ إذ نشير إلى أنه يمكننا بسهولة الالتفاف حول هذه المعضلة عن طريق وضع العدد $a$ المفقود في مقدمة القائمة $L$. وهذا يصنع القائمة $M$ الموسعة التي تحتوي على العدد المزعج $a$. مع ذلك، لم تختفِ المشكلة الأساسية؛ إذ يمكننا تطبيق تعليمات كانتور مرة أخرى لتقديم عدد جديد $b$ الذي لا يتواجد في القائمة الجديدة $M$. ويمكننا بالطبع مواصلة زيادة أعضاء القائمة الحالية كما سبق لأي عدد من المرات، ولكن تبقى النقطة التي أشار إليها كانتور صحيحة. مع أنه بإمكاننا مواصلة تكوين قوائم تحتوي على أعداد إضافية تَغاضَيْنا عنها سابقًا، فإنه لا يمكن أبدًا أن توجد قائمة واحدة معيَّنة تتضمن كل الأعداد الحقيقية.

ومن ثم، فإن مجموعة الأعداد الحقيقية جميعها أكبر بشكلٍ ما من مجموعة الأعداد الصحيحة الموجبة كلها. وحتى لو كانت كلتاهما لا متناهيةً، فلا يمكن المقارنة بينهما بالطريقة نفسها التي تُقارَن بها قائمة الأعداد الزوجية بقائمة كل أعداد العد. وبالفعل، إذا طبَّقْنا برهان كانتور القطري على قائمة مفترضة تضمُّ كل الأرقام بين 0 و1، فإن العدد $a$ المفقود سوف يقع أيضًا ضمن هذا النطاق. ولذلك، فإننا نستنتج بالمثل أن هذه




شكل ٧-٢: عدد كانتور $a$ يختلف عن كل $a_k$ في المنزلة العشرية $k$.

المجموعة سوف تتحدى كل محاولة لوضعها بالكامل في قائمة. أَذْكر ذلك لأننا سوف نستفيد من هذه الحقيقة قريبًا.

تُعد نتيجة كانتور لافتةً للنظر على نحو أكبر بالنظر إلى حقيقة أنه يمكن وضع كثيرٍ من مجموعات الأعداد الأخرى داخل قائمة لا متناهية، بما في ذلك أعداد إقليدس اليونانية. يشتمل الأمر على بعض البراعة، ولكن بمجرد تعلُّم خدعتين، ليس من الصعب إيضاح أن الكثير من مجموعات الأعداد «قابلة للعد»، وهو المصطلح الذي نستخدمه لنشير إلى أن المجموعة يمكن وضعها في قائمة بالطريقة نفسها التي توضع بها أعداد العد. وخلاف ذلك، فإن المجموعة غير المتناهية يطلق عليها «غير قابلة للعد».

على سبيل المثال، فلنأخذْ مجموعة الأعداد الصحيحة كلها **Z**، التي تأتينا بصورة تلقائية كقائمة لا متناهية على نحو مضاعف. مع ذلك يمكننا إعادة ترتيبها في صفٍّ بنقطة البداية: 0، 1، 1−، 2، 2−، 3، 3− ... وعن طريق اقتران كل عدد صحيح موجب مع نظيره المعاكس، نضع قائمة يظهر فيها كل عدد صحيح؛ ولن يُفلت منها عدد.

والأكثر إثارة للدهشة أننا يمكننا القيام بالأمر نفسه مع الأعداد النسبية: ابدأ بالصفر، ثم ضع الأعداد النسبية التي يمكن كتابتها باستخدام أعداد لا تزيد عن $1$ (وهي $1$ و$-1$)، ثم الأعداد التي لا تتضمن أعدادًا أكبر من $2$ (وهي $2$، $-2$، $\frac{1}{2}$، $-\frac{1}{2}$)، ثم الأعداد التي تستخدم أعدادًا حتى $3$ فقط، وهكذا. وبهذه الطريقة يمكن ترتيب الكسور (الموجبة والسالبة والصفر) في متتالية تظهر فيها جميعًا وتقع في حيِّزها. ومن ثم فإن الأعداد النسبية أيضًا تُشكِّل مجموعة قابلة للعد؛ مثل أعداد إقليدس، وفي الواقع إذا تأمَّلنا مجموعة كل الأعداد التي تنشأ من الأعداد النسبية من خلال أخْذ الجذور بأي درجة، فإن المجموعة الناتجة تظل قابلة للعد. ويمكننا حتى تجاوُز هذا؛ فمجموعة الأعداد الجبرية كلها (التي ذُكِرَت لأول مرة في الفصل السادس) — وهي الأعداد التي تمثِّل حلولًا للمعادلة العادية كثيرة الحدود — تشكِّل مجموعة يمكن من حيث المبدأ نَظْمُها في قائمة لا متناهية؛ بمعنى أنه من الممكن وصف قائمة نظامية تتضمنها جميعًا. (برهان ذلك مُشابِه للبرهان الخاص بالأعداد النسبية.)

ما سَمَحْنا بحدوثه حالَ قَبول أي مفكوك عشري — عَرَضًا — هو فتْح الباب أمام ما يُعرف بالأعداد المتسامية؛ وهي الأعداد التي تتجاوز الأعداد التي تنشأ من هندسة إقليدس والمعادلات الجبرية العادية. يوضِّح لنا برهان كانتور أن الأعداد المتسامية موجودة، وإضافة لذلك، لا بد أنه يوجد عدد لا متناهٍ منها؛ إذ إنها لو كانت تشكِّل مجموعة منتهية فحسب، فإنه يمكن وضعها في مقدمة قائمة الأعداد الجبرية لدينا (الأعداد غير المتسامية)؛ لذلك فإنَّ وضْع قائمة تتضمن كل الأعداد الحقيقية التي نَعْرفها الآن أمر مستحيل. واللافت للنظر أننا اكتشفنا وجود هذه الأعداد الغريبة دون تحديد عدد واحد منها! فقد كُشف وجودها ببساطة عن طريق مقارنة مجموعات لا متناهية بعضها ببعض. والأعداد المتسامية هي الأعداد التي تملأ الفراغ الكبير بين الأعداد الجبرية المألوفة ومجموعة كل المفكوكات العشرية، وباستخدام استعارةٍ من عِلم الفلك، فإن الأعداد المتسامية هي المادة المظلمة في عالم الأعداد.

وبالانتقال من الأعداد النسبية إلى الأعداد الحقيقية، فنحن ننتقل من مجموعة إلى مجموعة أخرى تَتَّسم بامتلاك «أعداد أصلية أعلى»، كما يُطلِق عليها علماءُ الرياضيات. وتتسم المجموعتان بهذه الصفة نفسها إذا كان يمكن قِران عناصرهما؛ عنصرًا لعنصر. وما يمكن إيضاحه باستخدام برهان كانتور هو أنَّ أيَّ مجموعة تتسم بامتلاك أعداد أصلية أقل من المجموعة التي تشكَّلتْ من كلِّ مجموعاتها الفرعية. وهذا أمر بديهي

بالنسبة للمجموعات المنتهية، وفي الواقع لقد أَوْضحنا في الفصل الخامس أنه إذا كان لدينا مجموعة من العناصر $n$، فإنه يوجد $2^n$ مجموعة فرعية يمكن تكوينهما بهذه الطريقة. ولكن ما مدى كِبر حجم المجموعة $S$ المتضمِّنة لكل المجموعات الفرعية للمجموعة غير المتناهية التي تضم الأعداد الطبيعية $\{1, 2, 3, \dots\}$؟ هذا السؤال ليس مثيرًا للاهتمام في حد ذاته فحسب، ولكن أيضًا في الطريقة التي نصل بها إلى الإجابة؛ وهي أن $S$ بالفعل غير قابلة للعد.

## متناقضة راسل

لنفترض على العكس أن $S$ نفسها قابلة للعد، وفي هذه الحالة يمكن إدراج المجموعات الفرعية لأعداد العد بترتيبٍ ما مثل $A_1, A_2, \dots$. والآن يمكن لعدد عشوائي $n$ أن يكون، أو لا يكون، عنصرًا من $A_n$؛ لنفترض المجموعة $A$ التي تتضمن كل الأعداد $n$ بحيث لا يكون $n$ عنصرًا في المجموعة $A_n$. والآن $A$ مجموعة فرعية لأعداد العد (ربما المجموعة الفرعية الفارغة) ومن ثم تظهر في القائمة المذكورة سابقًا في مكانٍ ما، مثلًا $A = A_j$. ويُطرح الآن سؤال ليس له إجابة: هل $j$ عنصر في $A_j$؟ إذا كانت الإجابة «نعم»، فمن واقع طريقة تعريف $A$ نفسها، نستنتج أن $j$ ليس عنصرًا في $A$، ولكن $A = A_j$؛ لذلك فهي تُناقِض نفسها. الإجابة البديلة هي لا، $j$ ليس عنصرًا في $A_j$، وفي هذه الحالة، مرة أخرى من خلال تعريف $A$، نستنتج أن $j$ عنصر في $A = A_j$، ومرة أخرى يكون لدينا تَناقُض. نظرًا لأن التناقض لا مفر منه، فلا بد أن افتراضنا الأصلي بأن المجموعات الفرعية لأعداد العد يمكن إدراجها على نحوٍ يجعلها قابلة للعد افتراضٌ خاطئ. وفي الواقع، ينجح هذا البرهان في إظهار أن مجموعة كل المجموعات الفرعية لأي مجموعة قابلة للعد — لكنها لا متناهية — هي مجموعة غير قابلة للعد.

قدم برتراند راسل (١٨٧٢–١٩٧٠) هذا البرهان المميز — الذي يَتبع أسلوب المرجعية الذاتية — في سياقٍ مختلفٍ قليلًا أدَّى إلى ما يُعرف باسم «متناقضة راسل». وقد طبَّقها راسل على «مجموعة كل المجموعات التي ليست عناصر في نفسها»، طارحًا السؤال المحرج عما إذا كانت هذه المجموعة عنصرًا في نفسها أم لا. ومرةً أخرى الإجابةُ «نعم» تقتضي ضمنًا «لا» والإجابة «لا» تقتضي ضمنًا «نعم»؛ مما أجبر راسل على استنتاج أن هذه المجموعة لا يمكن أن تكون موجودة.

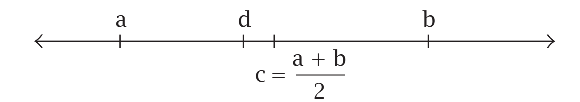
في تسعينيات القرن التاسع عشر، اكتشف كانتور نفسُه تَناقضًا ضمنيًّا ينبع من فكرة «مجموعة كل المجموعات». وأَقرَّ راسل بالفعل بأن برهان متناقضتِه مستلهَم من عمل كانتور. مع ذلك، فإن ثمرة كل هذا هي أننا لا يمكن أن نتخيل ببساطةٍ أن المجموعات الرياضية يمكن تقديمها بأي طريقة كانت، ولكنْ يجب وضع بعض القيود على طريقة تحديد المجموعات. ومنذ ذلك الحين يجتهد منظِّرو المجموعات ومتخصصو المنطق في التعامل مع تبعات ذلك. ويَظهر الحل الأكثر إرضاءً لهذه المشكلات في نظرية زيرميلو–فرانكل للمجموعات ومسلمة الاختيار.

## خط الأعداد تحت المجهر

توجد طرق مختلفة للنظر إلى حجم المجموعات غير المتناهية من الأعداد التي تنكشف إذا نظرْنا إلى توزيع أنواع الأعداد المختلفة التي تترابط معًا لِتُحوِّل خط الأعداد إلى متسلسلة. قد لا تكون الأعداد النسبية سوى مجموعةٍ من الأعداد قابلةٍ للعد، ولكن المجموعة متراكمةٌ على خط الأعداد بكثافة، بطريقة لا تتراكم بها الأعداد الصحيحة بكل وضوح. فَبِفرض وجود أي عددين مختلفين $a$ و$b$، فهناك عدد نسبي يقع بينهما. وبالتأكيد إن متوسط العددين $c = \frac{a+b}{2}$ عدد يقع بينهما، ولكن قد يكون عددًا غير نسبي. مع ذلك إذا كان $c$ عددًا غير نسبي، يمكننا أن نُقرِّبَه عن طريق العدد النسبي $d$، بمفكوك عشري غير متكرر، من خلال السماح لـ $d$ بأنه يكون له التمثيل العشري نفسه مثل $c$، وصولًا إلى عدد كبير للغاية من المنازل العشرية. على سبيل المثال، إذا كان $\sqrt{2} = 1.414\ldots$، فإن $\sqrt{2}$ يختلف عن $1.414$ بأقل من $0.001$، وفي كل مرة نحصل على منزلة عشرية أخرى، نضمن اكتشاف عدد نسبي يقترب من $\sqrt{2}$ بدقة أكبر (تبلغ في المتوسط عشرة أضعاف) من العدد السابق. وإذا كان عدد المنازل العشرية الأولى — التي يتفقان فيها — كبيرًا بما يكفي، فإن الفارق بينهما سوف يكون صغيرًا للغاية، لدرجة أن $c$ و$d$ كليهما سوف يقعان بين $a$ و$b$. ولسوف يعتمد عدد المنازل العشرية التي يَلزم الحصول عليها بَعد العلامة العشرية على مدى اقتراب $a$ و$b$ أحدهما من الآخر كبداية، ولكنْ دائمًا من الممكن إيجاد عدد نسبي $d$ يؤدي هذه المهمة (انظر شكل ٧-٣). فمجموعة الأعداد النسبية كثيفة على خط الأعداد لهذا السبب فحسب. وبالطبع نستطيع أن نبين — بالبرهان نفسه — أنه يوجد عدد نسبي آخر يقسم المسافة بين $a$ و$d$ مثلًا، وبهذه الطريقة نصل إلى استنتاج أن أعدادًا نسبية كثيرة ولا متناهية تقع بين أي عددين، بِغَضِّ النظر عن صغر

الفارق بين هذين العددين. وعلى نحو خاص لا يوجد شيء يسمى أصغر كسر موجب؛ إذ إنه بالنسبة لأي عدد موجب، يوجد دائمًا عدد نسبي يقع بينه وبين الصفر.

ما يعزز موقف مجموعة الأعداد غير النسبية أيضًا كَوْنُها مجموعةً كثيفة. وقبْل شرح ذلك، أشيرُ إلى أنه بمجرد تحديد عدد غير نسبي واحد — على سبيل المثال العدد الفيثاغورسي $\sqrt{2}$ — يصبح من الممكن على الفور تحديد المزيد على نحو لا متناهٍ. وعندما نجمع عددًا غير نسبي مع عدد نسبي، فإن الناتج دومًا ما يكون عددًا غير نسبي. على سبيل المثال، $\sqrt{2} + 7$ عدد غير نسبي بفضل هذه الحقيقة. وبطريقة مشابهة، إذا ضربنا عددًا غير نسبي في عدد نسبي (غير الصفر)، فإن الناتج يكون عددًا غير نسبي آخر. (يُبرهِن على هذين الزعمين حُجَّتا تَناقُضٍ بسيطتان.) وعلى وجه الخصوص، يمكننا أن نجد عددًا غير نسبي صغيرًا بالقدر الذي نرغب فيه؛ حيث $t = \frac{\sqrt{2}}{n}$ عدد غير نسبي لأيٍّ من أعداد العد $n$، وبجعل $n$ أكبر وأكبر، يمكننا جعل $t$ أقرب إلى الصفر كما نشاء، وكما هي الحال مع الأعداد النسبية ندرك أنه لا يوجد أصغر عدد غير نسبي موجب؛ ومن ثم فلا يوجد ما يطلق عليه أصغر عدد موجب.




شكل ٧-٣: الأعداد النسبية توجد بين أي موضعين على خط الأعداد.

بالعودة إلى أرقامنا $a$ و$b$، افترضْ مرة أخرى أن $c$ يمثل متوسطهما. فإذا كان $c$ غير نسبي، يكون لدينا عدد من النوع المطلوب (غير نسبي). على الجانب الآخر، إذا كان $c$ عددًا نسبيًّا، فضَعْ $d = c + t$؛ حيث $t$ هو العدد غير النسبي الذي تَحدَّثْنا عنه الفقرة السابقة. ووفقًا لما حدث من قبل، فإن $d$ سوف يكون أيضًا غير نسبي، وإذا افترضنا أن $n$ كبير على نحو كافٍ، يمكننا دومًا أن نضمن أن $d$ قريب للغاية من المتوسط $c$ للعددين $a$ و$b$ وأنه يقع بينهما. وبهذه الطريقة ندرك أن الأعداد غير النسبية أيضًا تُشكل مجموعة كثيفة، ويمكننا — على غرار الأعداد النسبية — أن نستنتج أنه يوجد الكثير من الأعداد غير النسبية على نحو لا متناهٍ تقع بين أي عددين على خط الأعداد.

وهكذا، فمجموعة الأعداد النسبية ومكملتها مجموعة الأعداد غير النسبية متماثلتان من ناحية (فكلتاهما كثيفة على خط الأعداد)، ومن ناحية أخرى ليستا متماثلتين (فالمجموعة الأولى قابلة للعد بينما الثانية غير قابلة للعد).

## مجموعة الثلث الأوسط لكانتور

لدينا الآن فكرة أكثر وضوحًا عن طريقة تضافُر الأعداد النسبية وغير النسبية لتشكيل خط الأعداد الحقيقية. وتشكِّل الأعدادُ النسبية مجموعةً قابلة للعد، مع ذلك تتراكم بكثافة على خط الأعداد. وعلى النقيض من ذلك، مجموعةُ الثلث الأوسط لكانتور هي مجموعة فرعية غير قابلة للعد لفترة الوحدة التي — مع ذلك — تتناثر على نحو خفيف؛ وهي نتيجة البنية التالية.

نبدأ بفترة الوحدة $I$، وهي تمثل كل الأعداد الحقيقية من صفر حتى 1 وتشمل 1 أيضًا. الخطوة الأولى في تكوين مجموعة كانتور هي إزالة الثلث الأوسط من هذه الفترة، وهي كل الأعداد بين $\frac{1}{3}$ و$\frac{2}{3}$. وتتضمن المجموعة الباقية فترتين من صفر حتى $\frac{1}{3}$ ومن $\frac{2}{3}$ حتى 1. وفي المرحلة الثانية، نتخلص من الثلث الأوسط لهاتين الفترتين، وفي المرحلة الثالثة، نتخلص من الثلث الأوسط للفترات الباقية، وهكذا. وبعد ذلك، ستحتوي مجموعة الثلث الأوسط لكانتور $C$ على كل نقاط $I$ التي لم تُحذف في أي مرحلة من هذه العملية.

$0$ $1$

$\frac{1}{3}$ $\frac{2}{3}$

$\frac{1}{9}$ $\frac{2}{9}$ $\frac{7}{9}$ $\frac{8}{9}$

$\frac{1}{27}$ $\frac{2}{27}$ $\frac{7}{27}$ $\frac{8}{27}$ $\frac{19}{27}$ $\frac{20}{27}$ $\frac{25}{27}$ $\frac{26}{27}$

شكل ٧-٤: تطور مجموعة الثلث الأوسط لكانتور إلى المستوى الرابع.

يبلغ إجمالي طول الفترات الصغيرة التي تتبقى كلما انتقلنا من مرحلة لأخرى في هذه العملية — عمدًا — $\frac{2}{3}$ المرحلة السابقة؛ وينتج عن ذلك أنه في المرحلة $n$، يبلغ

إجمالي طول الفترات المتبقية $(\frac{2}{3})^n$. ويصل هذا التعبير الجبري إلى الصفر كلما زاد $n$، ونظرًا لأن مجموعة كانتور $C$ هي مجموعة كل النقاط التي تتبقى في نهاية هذه العملية بأكملها، فإن «طول» أو قياس $C$ لا بد أن يكون صفرًا.

ربما نَشكُّ أننا تَخلَّصْنا من كل النقاط ولم يَعُدْ هناك نقاط باقية في $C$. فهل مجموعة الثلث الأوسط تكون فارغة؟ الإجابة هي «لا» مدوية! هناك أعداد كثيرة على نحو لا متناهٍ متبقية في $C$. ويتضح هذا على نحو أفضل إذا نقلنا تمثيلنا لأعداد فترة الوحدة إلى الكسور العشرية ذات الأساس 3 المعروفة باسم «الأعداد الثلثية»؛ حيث تعتمد البنية بأكملها على 3. ففي الكسور العشرية ذات الأساس 3، يُمثل العددان $\frac{1}{3}$ و$\frac{2}{3}$ على الترتيب بالصيغة 0.1 و0.2. وعن طريق التخلص من الثلث الأوسط من فترة الوحدة، نتخلص من كل الأعداد التي يبدأ مفكوكها العشري الثلثي بـ 0.1، وبالفعل تتخلص العملية الكلية بالضبط من كل الأعداد التي تشتمل على 1 في أي منزلة في مفكوكها الثلثي. والأعداد الموجودة في $C$ هي بالضبط الأعداد التي تشتمل مفكوكاتها الثلثية على صفر و2. (على سبيل المثال، ينجو العدد $\frac{3}{4}$ من عملية التخلص غير المتناهية من الأعداد؛ إذ إن مفكوكه الثلثي يشتمل على الجزء المتكرر $0.202020\ldots$.)

بعد ذلك، نلاحظ معًا أمرًا مدهشًا. من خلال أخذ المفكوك الثلثي لأي عدد $c$ في المجموعة $C$ واستبدال 1 بكل 2، نحصل على المفكوك الثنائي لعدد ما $c'$ في فترة الوحدة. وهذا يعني وجود توافق بين $C$ ومجموعة كل الأعداد في $I$ (المكتوبة بالأساس الثنائي)، الذي يعني بدوره أن الأعداد الأصلية في $C$ هي نفس الأعداد الأصلية في $I$، ونظرًا لأن $I$ مجموعة غير قابلة للعد (ببرهان كانتور القطري)، فإن مجموعة الثلث الأوسط لكانتور ليست مجموعة لا متناهية فحسب، بل غير قابلة للعد أيضًا.

ومن ثَم، فإن لدينا مجموعة $C$ التي يمكن إهمالها — من جهة — من حيث الحجم (إذ يبلغ قياسها صفرًا)، ولكن بطريقة حساب أخرى، تعد المجموعة $C$ ضخمة؛ لأنها تشمل الأعداد الأصلية نفسها التي تشتمل عليها المجموعة $I$؛ ومن ثم الأعداد التي يشتمل عليها خط الأعداد الحقيقية بأكمله.

الأدهى من ذلك أن $C$ ليست كثيفة في أي منزلة، بل العكس تمامًا. تذكَّرْ أننا نَعني بقولنا إن مجموعةً على غرار الأعداد النسبية كثيفةٌ، أنه حينما نأخذ عددًا حقيقيًّا $a$، فإنه لا بد من وجود أعداد نسبية في أي فترة صغيرة محيطة بالعدد $a$، مهما بلغ صِغَر هذه الفترة؛ فنقول إن أي مساحة مجاورة للعدد $a$ تتضمن عناصر من مجموعة الأعداد

النسبية. ولكن تتمتع مجموعة كانتور بالطبيعة النقيضة تمامًا لذلك؛ فالأعداد التي لا توجد في المجموعة $C$ ربما توجد على خط الأعداد دون الالتقاء بأي عنصر من $C$، شريطة أن تقتصر خبراتها على مساحة صغيرة للغاية حول المكان الذي تتواجد فيه. للتعرف على ذلك خذ أي عدد $a$ ليس عنصرًا في $C$، بحيث يحتوي مفكوك العدد $a$ الثلاثي على 1 مرة واحدة على الأقل: $a = 0 \ldots 1 \ldots,$، ويكون 1 في المنزلة العشرية $n$ مثلًا. فبالنسبة للفترة الصغيرة على نحو كافٍ المحيطة بالعدد $a$، فإن الأعداد $b$ في هذه الفترة يكون لها مفكوك ثلثي يتفق مع مفكوك $a$ الثلثي، حتى في منازل تتخطى المنزلة $n$؛ ومن ثم فإن الأعداد كلها أيضًا لن تكون عناصر في المجموعة الغريبة $C$؛ إذ إن مفكوكاتها الثلثية سوف تحتوي على الأقل على ظهور واحد للعدد 1.

على الجانب الآخر، أي عنصر $a$ في مجموعة كانتور لن يشعر بعزلة شديدة؛ إذ إن $a$ عندما يبحث في أي فترة $J$ تحيط به على خط الأعداد — مهما كانت صغيرة — سوف يجد $a$ جيرانًا من المجموعة $C$ بجواره (إلى جانب إيجاد أعداد ليست من المجموعة $C$ أيضًا). ويمكننا تحديد عنصر $b$ في الفترة المذكورة $J$ يقع أيضًا في المجموعة $C$ عن طريق افتراض أن $b$ له مفكوك ثلثي يتفق مع $a$ في عدد كبير على نحو كافٍ من المنازل العشرية، ولكن دون اشتمال أيٍّ منها على 1. وفي الواقع يوجد عدد كبير لا يمكن حصره من عناصر $C$ في $J$.

في الختام، إن مجموعة الثلث الأوسط لكانتور وفيرة العدد لأقصى حد ممكن، والعناصر الموجودة في المجموعة $C$ تستطيع مقابلة عناصر أخرى ذات صلة في أي مكان تبحث فيه. ومع ذلك، فبالنسبة للأعداد التي ليست عناصر في $C$، فإن المجموعة $C$ لا تكاد تكون موجودة على الإطلاق. فلا يمكن تحديد أحد عناصر $C$ في الأماكن الحصرية للأعداد التي ليست عناصر في $C$، كما أن قياس المجموعة $C$ نفسها يبلغ صفرًا. فبالنسبة لها، $C$ ليس لها وجود كالعدم.

## المعادلات الديوفانتية

ربما تُمثَّل بعض المجموعات الرئيسية الموجودة على خط الأعداد بلغة المعادلات. والأعداد النسبية — التي تشكِّل مجموعة قابلة للعد — هي الأعداد التي تَظهر كحلول للمعادلات الخطية البسيطة: الكسر $\frac{b}{a}$ هو حل المعادلة $ax - b = 0$ ($a$ و$b$ عددان صحيحان). والأعداد على غرار $\sqrt{2}$، والتي لا تظهر بهذه الطريقة، يُطلق عليها أعداد غير نسبية،

وتشكِّل مجموعة غير قابلة للعد لا يمكن إقرانها بأعداد العد مثلما نستطيع فعل ذلك مع الأعداد النسبية. وضمن مجموعة الأعداد غير النسبية توجد الأعداد المتسامية، وهي الأعداد التي لا تَظهر أبدًا كحلول لهذا النوع من المعادلات، حتى لو استخدمنا قوًى أعلى للعدد $x$. ومن المعروف أن $\pi$ مثال على الأعداد المتسامية، ولكن $\sqrt{2}$ ليس مثالًا عليها؛ إذ إنه يحل المعادلة $x^2 - 2 = 0$. ومن ثم فإن المنهج المتبع هنا هو تعريف فئات الأعداد من خلال أنواع المعادلات التي تحلها.

مع ذلك، يَبرز اتجاه مثير من الدراسة عندما نسلك السبيل المعاكس ونُصِرُّ على أنه ليست معاملات معادلاتنا فحسب هي التي ينبغي أن تكون أعدادًا صحيحة، ولكن حلول المعادلات أيضًا. إليك مثالًا تقليديًّا على ذلك.

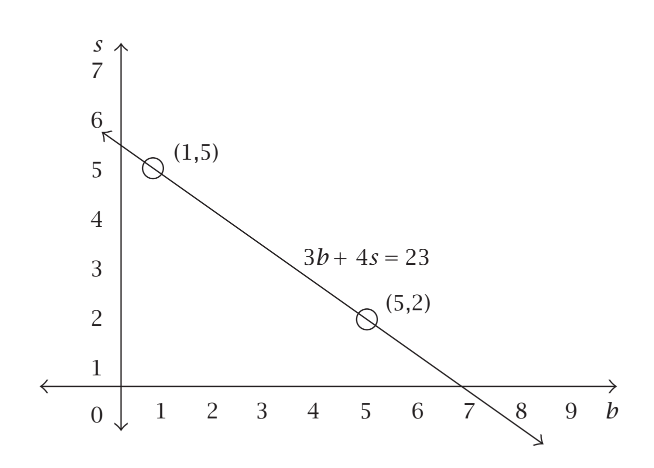
«يحتوي صندوق على عناكب وخنافس و46 ساقًا، كم عدد كل نوع من المخلوقات في هذا الصندوق؟» يمكن حل لغز الأعداد البسيط هذا بسهولة بالمحاولة، ولكن من المفيد ملاحظة أنه أولًا: يمكن تمثيله بمعادلة: $6b + 8s = 46$، وثانيًا: أننا مهتمون فحسب بأنواع معينة من الحلول لهذه المعادلة؛ وهو أن عدد الخنافس $b$ وعدد العناكب $s$ من أعداد العد. وبوجه عام، يطلق على نظام من المعادلات اسم «المعادلات الديوفانتية»، عندما نَقْصُر بحثنا عن الحلول على نوع معين من الأعداد، وعادةً ما نبحث عن حلول من الأعداد الصحيحة أو النسبية.

توجد طريقة بسيطة لحل المعادلات الديوفانتية الخطية مثل تلك المعادلة. أولًا، اقسم المعادلة على القاسم المشترك الأكبر للمعاملين، اللذين هما في هذه الحالة 6 و8؛ وبذا فالقاسم المشترك الأكبر لهما هو 2. وبإلغاء هذا العامل المشترك 2، نحصل على معادلة مكافئة؛ أي معادلة لها الحل نفسه: $3b + 4s = 23$. إذا لم يَعُد الطرف الأيمن من المعادلة عددًا صحيحًا بعد إجراء هذه القسمة، فهذا يعلمنا أنه لا يوجد حلول من أعداد صحيحة لهذه المعادلة، وأننا يمكننا أن نتوقف عند هذا الحد. الخطوة التالية هي أخذ أحد المعاملين، وعادة ما يكون الأصغر هو الأسهل، والعمل على مضاعفاته، وفي هذه الحالة هو 3. ويمكن كتابة معادلتنا بهذا الشكل: $3b + 3s + s = (3 \times 7) + 2$؛ وبإعادة الترتيب نحصل على $s = (3 \times 7) - 3b - 3s + 2$. الهدف من هذا هو إيضاح أن $s$ لها الشكل $3t + 2$ للعدد الصحيح $t$. وبالتعويض بـ $s = 3t + 2$ في معادلتنا وجعْل $b$ الطرف الرئيسي في المعادلة، نحصل على:

$$3b + 4(3t + 2) = 23 \Longrightarrow 3b = 15 - 12t \Longrightarrow b = 5 - 4t.$$

لدينا الآن الحل الكامل للمعادلة الديوفانتية بالأعداد الصحيحة: $b = 5 - 4t, s = 3t + 2$. واختيار أي قيمة بعدد صحيح لـ $t$ سوف يحل المعادلة، وكل الحلول بالأعداد الصحيحة تكون على هذه الصيغة.

مع ذلك، فإن مسألتنا الأصلية مقيدة بقدر أكبر من ذلك؛ حيث إنه يجب ألا يقل $b$ و$s$ عن صفر؛ إذ لا يوجد خنافس أو عناكب سالبة. وبذلك، فإنه لا يوجد إلا قيمتان ممكنتان لـ $t$، وهما $t = 0$ و$t = 1$؛ مما يقدم الحلَّين المحتملين: 5 خنافس وعنكبوتان، وخنفسة واحدة و5 عناكب. وإذا فسرنا اللغز على أنه يوجد مجموعة من كلا النوعين، نحصل على الحل التقليدي: 5 خنافس وعنكبوتان.




شكل ٧-٥: النقاط الشبكية على خط المعادلة الخطية.

يسمى هذا النوع من المسائل «مسائل خطية»؛ لأن الرسم البياني للمعادلة المصاحبة له يتكون من خط لا متناهٍ من النقاط. وعلى المسألة الديوفانتية إيجاد «النقاط الشبكية» على هذا الخط، وهي النقاط التي يتكامل فيها كلا الإحداثيَّين، أو النقاط الشبكية في الربع الموجب فقط إذا كنَّا نسمح فحسب بالحلول الموجبة.

مع ذلك، فبمجرد إدخال التربيع والقوى الأعلى في معادلاتنا، فإن طبيعة المسائل المقابلة تختلف اختلافًا أكبر وتزداد إثارة. إحدى المسائل التقليدية على هذا النوع التي

لها حل كامل تتعلق بإيجاد كل «ثلاثيات فيثاغورس»: وهي الأعداد الصحيحة الموجبة $a$ و$b$ و$c$؛ حيث $a^2 + b^2 = c^2$. وبالطبع، استَقَتْ ثلاثياتُ فيثاغورس اسمَها من حقيقة أنها تسمح لك بِرَسم مثلث قائم الزاوية بأضلاع يبلغ طولها هذه الأعداد الصحيحة. المثال التقليدي على هذا هو المثلث (3، 4، 5). فبوجود أي ثلاثي فيثاغورسي، يمكننا إنتاج المزيد ببساطة بمضاعفة كل أعداد الثلاثي في أي عدد موجب؛ إذ ستتواصل المعادلة الفيثاغورسية دون توقف. على سبيل المثال، يمكننا مضاعفة المثال السابق لنحصل على الثلاثي (6، 8، 10). مع ذلك، يعطي هذا الثلاثي مثلثًا مماثلًا — يتضمن النِّسَب نفسها — إذ إن التغيير مجرد تغيير في الحجم وليس في الشكل. وبالنظر إلى المثلث الأول نجد الثلاثي الثاني ببساطة من خلال قياس أطوال الأضلاع بوحدات تساوي نصف حجم الوحدات الأصلية؛ ومن ثم مضاعفة الحجم العددي للأبعاد. مع ذلك، توجد ثلاثيات مختلفة حقًّا مثل التي تُمثلها المثلثات قائمة الزاوية ذات الأبعاد (5، 12، 13) و(65، 72، 97).

لذلك، من أجل التعبير عن كل ثلاثيات فيثاغورس، يكفي أن نفعل ذلك مع كل الثلاثيات $(a, b, c)$؛ حيث يكون القاسم المشترك الأكبر بين الثلاثة هو 1؛ إذ إن كل الثلاثيات الأخرى ما هي إلا نُسَخ مكبَّرة من هذا الثلاثي. وطريقة القيام بذلك هي كالتالي: خذ أي عددين صحيحين موجبين أوليَّين فيما بينهما $m$ و$n$، أحدهما زوجي، ولنجعل $m$ أكبرهما. شكِّل الثلاثي المحدد عن طريق $a = 2mn$، و$b = m^2 - n^2$، و$c = m^2 + n^2$. وعندها سيمثل الأعداد الثلاثة $a$ و$b$ و$c$ ثلاثيًّا فيثاغورسيًّا (ومن السهل التأكد من الحسابات الجبرية)، وليس بين الأعداد الثلاثة أي عامل مشترك (ولا يصعب التأكد من ذلك أيضًا). وتنشأ الأمثلة الثلاثة السابقة من خلال اعتبار $m = 2$ و$n = 1$ في الحالة الأولى، و$m = 3$ و$n = 2$ في الحالة الثانية، بينما في المثلث الأخير لدينا $m = 9$ و$n = 4$. ويتطلب التحقق من العكس مزيدًا من الجهد؛ فأي ثلاثي فيثاغورسي مشابه ينشأ بهذه الطريقة باستخدام قيم مختارة على نحو مناسب للعددين $m$ و$n$. وعلاوة على ذلك، فإن التمثيل فريد من نوعه؛ إذ إن زوجين مختلفين من ($m$ و$n$) لا يمكن أن ينتجا الثلاثي نفسه $(a, b, c)$.

ليس للمعادلة المقابلة الخاصة بالأعداد المكعبة والقوى العليا حلٌّ على الإطلاق: فَلِأَيِّ قوة $n \geq 3$، لا يوجد ثلاثي صحيح موجب $x$ و$y$ و$z$؛ حيث يكون $x^n + y^n = z^n$. هذه هي «مبرهنة فيرما الأخيرة»، التي ربما ستُعرف في المستقبل باسم «مبرهنة وايلز»؛

إذ ثَبَتَت مصداقيتها أخيرًا في تسعينيات القرن العشرين على يد السير أندرو وايلز. وحتى بالنسبة لحالة الأعداد المكعبة — التي حُلَّت لأول مرة عن طريق أويلر — فإنها مسألة صعبة للغاية. مع ذلك، فمن السهل نسبيًّا إيضاح أن حاصل جمع عددين مرفوعين للقوة الرابعة لا يكون عددًا مربعًا أبدًا (وبالطبع ليس عددًا مرفوعًا للقوة الرابعة أيضًا). وهذا كافٍ لقَصْر المسألة على الحالة التي يكون فيها $n$ عددًا أوليًّا $p$ (ما يعني أنه إذا حلَّلنا المسألة لكل الأسس الأولية، فإن النتائج العامة سوف تتبع ذلك على الفور)، وبالفعل حُلَّت المسألة بالنسبة لما يُطلق عليه الأعداد الأولية النظامية في القرن التاسع عشر. مع ذلك، تَحقَّق الحل الكامل فقط كنتيجة لحل وايلز لمسألة عميقة يُطلَق عليها «حدسية شيمورا وتانياما».

مع ذلك، فالمعادلة الديوفانتية التي حظيتْ بالدراسة المكثفة هي معادلة بِل $x^2 - ny^2 = 1$؛ حيث $n$ عدد صحيح موجب ليس مربعًا. ولقد أُدركَتْ أهميتها في زمن مبكر للغاية؛ إذ يبدو أنها خضعت للدراسة في اليونان والهند، ربما في عام ٤٠٠ قبل الميلاد؛ لأن حلها يعطي تقريبات نسبية جيدة $\frac{x}{y}$ للعدد $\sqrt{n}$. على سبيل المثال، عندما يكون $n = 2$، يكون للمعادلة — كأحد أزواج الحلول — العددان $x = 577$ و$y = 408$ إلى جانب $(\frac{x}{y})^2 = 2.000006$. وترتبط المعادلة بالعملية الهندسية التي كان الإغريق يُطلِقون عليها اسم «الطرح المستمر»؛ حيث تبدأ بقطعتين مستقيمتين وتُواصل طرح الأقصر من الأطول، وهي نوعٌ مُناظِر لخوارزمية إقليدس، ولكن تنطبق على أطوال متواصلة. وفي الواقع، تؤدي معضلة الماشية لأرخميدس — المذكورة في الفصل الخامس — لصورة من معادلة بِل.

خضعتْ صور من معادلة بِل للدراسة على يد ديوفانتوس نفسه في قرابة عام ١٥٠ ميلادية، وحلها عالم الرياضيات الهندي العظيم براهما جوبتا (عام ٦٢٨)، وتحسنت طرق حلها على يد بهاسكارا الثاني (عام ١١٥٠)، الذي أوضح كيفية الحصول على حلول جديدة من حلٍّ أوَّلي. وفي أوروبا، كان فيرما هو الذي حثَّ علماءَ الرياضيات على تحويل انتباههم إلى معادلة بِل، ونُسبَت النظرية الكاملة إلى عالم الرياضيات الفرنسي الشهير جوزيف لوي لاجرانج (١٧٣٦–١٨١٣) (أما عن التسمية الإنجليزية «بِل» فهي مصادفة تاريخية). وتعتمد طريقة الحل العامة على المفكوك العشري المستمر لـ $\sqrt{n}$.

## فيبوناتشي والكسور المستمرة

تَذكَّرْ متتالية الأعداد 1، 1، 2، 3، 5، 8، 13، 21 ... التي اكتشفها فيبوناتشي، والمذكورة في الفصل الخامس، وخذْ زوجًا من الحدود المتتابعة في هذه المتتالية، واكتبِ النسبة المقابلة له في صورة واحد وكسر. والآن، إذا طبَّقْنا الأسلوب المصري على هذا الكسر عن طريق قسمة البسط والمقام على البسط، فسوف يظهر نمط مذهل. خذ مثالًا على ذلك:

$$\frac{13}{8}=1+\frac{5}{8}=1+\frac{1}{1+\frac{3}{5}}=1+\frac{1}{1+\frac{1}{1+\frac{2}{3}}}=1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1+\frac{1}{1}}}}}.$$

سوف نحصل على كسر متعدد الأدوار يتكون بأكمله من أعداد 1، وتظهر النِّسب السابقة لأعداد فيبوناتشي كلما تعمقنا في الحساب. ويجب أن يحدث ذلك في كل مرة، فمن خلال طريقة تحديد هذه الأعداد، فإن كل عدد فيبوناتشي يقل عن ضِعف التالي له؛ ومن ثم فإن نتيجة القسمة ستكون 1 وسيكون الباقي هو عدد فيبوناتشي السابق. وسوف تتذكر أن نسبة أعداد فيبوناتشي المتتالية تقترب من النسبة الذهبية $\tau$، وهكذا يشير ذلك إلى أن $\tau$ هي القيمة النهائية للكسر المستمر المكون بالكامل من أعداد 1.

كما أوضحنا في الفصل الخامس، فإن قيمة أي عملية متكررة لا متناهية يمكن جعلها الطرف الرئيسي لمعادلة تعتمد على هذه العملية. فإذا أطلقنا على قيمة البرج الكسري غير المتناهي المكوَّن من العدد 1 اسم $a$، نجد أن $a$ يعوض العلاقة $a=1+\frac{1}{a}$؛ لأن ما يقع أسفل الدور الأول للكسر هو مجرد نسخة جديدة من $a$. ومن هذا، نجد أن $a$ يعوض المعادلة التربيعية $a^2=a+1$، والجذر الموجب لها هو $\tau=\frac{1+\sqrt{5}}{2}$.

نوع الكسور المستمرة الناتج عن هذه العملية مهم في حد ذاته. فعندما نقرِّب عددًا غير نسبي $y$ عن طريق الأعداد النسبية، ننتقل بالطبع إلى التمثيل العشري للعدد $y$. وهذا ممتاز للحسابات العامة، ولكنَّ كَوْن العدد مرتبطًا بأساس معين ليس أمرًا طبيعيًّا على المستوى الرياضي. وكذلك من الضروري لطبيعة العدد $y$ مدى دقة تقريب العدد $y$ عن طريق الكسور ذات المقامات الصغيرة نسبيًّا. هل توجد طريقة لإيجاد متسلسلة من الكسور تتوافق على أفضل نحو مع المتطلبات المتناقضة لتقريب $y$ بدرجة عالية من الدقة، مع إبقاء المقامات صغيرة نسبيًّا؟ تكمن الإجابة في تمثيل الكسر المستمر للعدد، الذي يفعل ذلك من خلال اقتطاع الأدوار السفلية (المقام) دائمًا.

تبدو الكسور المستمرة غريبة للغاية بسبب الأدوار العديدة التي استخدمناها في تمثيلها. مع ذلك، يسهل تخطي إزعاج كتابة كل أدوار القسمة؛ فنظرًا لأن كل بسط يساوي 1، فلا نحتاج سوى تسجيل حاصل القسمة لتحديد الكسر المستمر الذي نقصده. على سبيل المثال، يتطور تمثيل الكسر $\frac{25}{91}$ بالطريقة التالية:

$$\frac{25}{91} = 0 + \frac{1}{3 + \frac{16}{25}} = 0 + \frac{1}{3 + \frac{1}{1+\frac{9}{16}}} = \cdots$$

والذي يَنتج في نهاية المطاف الكسرُ المستمر الذي حدَّدتْه القائمة $[0, 3, 1, 1, 1, 3, 2]$. وكما رأينا من قبل، النسبة الذهبية $\tau$ لها تمثيل الكسر المستمر $[1, 1, 1, 1, \ldots]$. ونكتب $\tau = [\overline{1}]$ بطريقة تُذَكِّرنا بالترميز العشري المتكرر. والظهور الأول للعدد 3 في الكسر المستمر $\frac{25}{91}$ يأتي من كتابة $91 = 3 \times 25 + 16$، وهو السطر الأول من خوارزمية إقليدس لزوج الأعداد (91، 25). وفي الواقع، لهذا السبب بالضبط يوجد سطر واحد في الكسر المستمر لكل سطر في الخوارزمية عند تطبيقها على العددين. وعلى نحو خاص، عند البدء بـ «كسر مختزل» — يكون فيه العددان أوليَّين فيما بينهما — سينطبق الأمر نفسه على كل الكسور التي تَنتج خلال حسابات الكسر المستمر المتوافق معها.

يفتح المثالُ الخاص — الناتج عن النسبة الذهبية — البابَ أمام فكرة أننا ربما نكون قادرين على تمثيل الأعداد الأخرى غير النسبية، باستخدام كسور مستمرة لا متناهية، وليس عن طريق كسور مستمرة متناهية (التي تمثل هي نفسُها أعدادًا نسبية على نحو واضح). ولكن كيف يَنتج الكسر المستمر للعدد $a$؟ سينبغي على القارئ السماح بقليل من الخدع الجبرية لرؤية تطبيق ذلك على الواقع، وإليك طريقة تنفيذه.

توجد خطوتان في عملية حساب الكسر المستمر للعدد $a = [a_0, a_1, a_2, \ldots]$. العدد $a_0$ هو الجزء الصحيح في العدد $a$، ويشار إليه $a_0 = \lfloor a \rfloor$. (على سبيل المثال، الجزء الصحيح من $\pi = 3.1415927\ldots$ ينتج عن $3 = \lfloor \pi \rfloor$.) وبوجه عام $a_n = \lfloor r_n \rfloor$؛ أي الجزء الصحيح في $r_n$؛ حيث يُعرف الحد الباقي $r_n$ بتكرار، على النحو $r_0 = a, r_n = \frac{1}{r_{n-1} - a_{n-1}}$. وعلى سبيل المثال، بتطبيق ذلك على $a = \sqrt{2}$ وباستخدام

الأداة الجبرية الخاصة بترشيد المقام (والتي ربما يَأْلَفُها بعض القراء) — نظرًا لأن $\lfloor \sqrt{2} \rfloor = 1$ — نحصل على:

$$a = r_0 = \sqrt{2} = 1 + (\sqrt{2} - 1),$$

بحيث $a_0 = 1$؛

$$r_1 = \frac{1}{r_0 - a_0} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{(\sqrt{2} - 1)(\sqrt{2} + 1)} = \sqrt{2} + 1,$$

$$a_1 = \lfloor r_1 \rfloor = 2.$$

وبعد ذلك نحصل على:

$$r_2 = \frac{1}{r_1 - a_1} = \frac{1}{(\sqrt{2} + 1) - 2} = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{(\sqrt{2} - 1)(\sqrt{2} + 1)}$$
$$= \sqrt{2} + 1,$$

بحيث تكون: $r_1 = r_2 = \cdots = \sqrt{2} + 1, a_1 = a_2 = \cdots = 2$، وهكذا فإن: $\sqrt{2} = [1, \overline{2}]$.

في الواقع، إنَّ الأعداد التي لها تمثيلات متكررة كالكسور المستمرة هي أعداد نسبية (هي — على نحو دقيق — الأعداد التي تتوقف تمثيلاتها عن التكرار)، كما أنها الأعداد التي تَنتج عن معادلات تربيعية على غرار $\tau$، التي قابلناها سابقًا هي حل للمعادلة $x^2 = x + 1$ و$\sqrt{2} = [1, \overline{2}]$، التي تعوض المعادلة $x^2 = 2$. وتوجد بعض الأمثلة التي توضح طبيعة عدم قابلية التكرارات للتنبؤ بها؛ منها: $\sqrt{3} = [1, \overline{1, 2}]$، و$\sqrt{7} = [2, \overline{1, 1, 1, 4}]$، و$\sqrt{17} = [4, \overline{8}]$، و$\sqrt{28} = [5, \overline{3, 2, 3, 10}]$. مع ذلك، فهناك جانب خاص ومميز للغاية في نمط مفكوك الكسر المستمر الخاص بالجذر التربيعي لعدد غير نسبي. يبدأ المفكوك بعدد صحيح $r$، ويتكون الجزء المتكرر من متتالية بَلِيندرومية (متتالية من الأعداد التي تُقرأ بالترتيب نفسه من الاتجاهين) يتبعها $2r$. ويمكن رؤية ذلك في كل الأمثلة السابقة، على سبيل المثال، بالنسبة للعدد $\sqrt{28}$، نجد أن $r = 5$، والجزء البَلِيندرومي في المفكوك هو 3، 2، 3، الذي يتبعه $2r = 10$. وبالنسبة للعددين $\sqrt{2}$ و$\sqrt{17}$، فإن الجزء البَلِيندرومي فارغ، ولكن لا يزال النمط موجودًا، ولو في صورة

بسيطة. فيمكن إيضاح أن التمثيل الكسري المستمر لعددٍ ما فريد من نوعه؛ إذ يحمل الكسران المستمران المختلفان قيمتين مختلفتين.

تعود أهمية الكسور المستمرة في تقريب الأعداد غير النسبية عن طريق أعداد نسبية إلى ما يطلق عليه «تقاربات» الكسر، وهي التقريبات النسبية للعدد الأصلي، التي تنتج عن اقتطاع التمثيل عند نقطة معينة وإيجاد العدد النسبي المقابل له. وهذا يمثل أفضل تقريب ممكن للعدد محل التقريب؛ بمعنى أن أي تقريب أفضل سوف يتضمن مقامًا أكبر من مقام التقاربات. وتقاربات النسبة الذهبية هي نسب فيبوناتشي. ونظرًا لأن كل حد في تمثيل الكسر المستمر للعدد $\tau$ هو $1$، فإن تقارب هذه النسب يُؤخر بأكبر قدر ممكن. ولهذا السبب، لا يوجد عدد أصعب من $\tau$ في التقريب بأعداد نسبية، ونِسَب فيبوناتشي هي أفضل تقريب يمكنك التوصل إليه.

إذا كان مقام تقارب الكسر المستمر هو $q$، فإن التقريب دائمًا ما يكون ضمن $\frac{1}{\sqrt{5}q^2}$ من القيمة الحقيقية للعدد، وتقلل تقارباتُ الكسر المستمر وتزيد القيمةَ التي تقترب منها بالتناوب. مع ذلك، فأسوأ الأعداد — عندما يتعلق الأمر بالتقريب بالأعداد النسبية — هي أعداد إقليدس مثل $\tau$ و$\sqrt{2}$. ومع ذلك، فإن بعض الأعداد المتسامية المعيَّنة — التي قد تبدو في طبيعتها أبعد ما تكون عن عالم الأعداد النسبية — ربما تُقرَّب على نحو شديد للغاية، ويكون لها تقاربات تتجه بسرعة كبيرة إلى العدد المنشود.

تتضح الصلة بمعادلة بِل $x^2 - ny^2 = 1$ — المذكورة في ختام الجزء السابق — بوجود الحل $(x, y)$ للمعادلة، مع أقل قيمة موجبة ممكنة للعدد $x$، ويمكن العثور على هذا الحل بين تقاربات التمثيل الكسري المستمر للعدد $\sqrt{n}$. على سبيل المثال، عندما يكون $n = 7$، فإن متتالية تقاربات $\sqrt{7}$ تبدأ بـ $2/1$، $3/1$، $5/2$، $8/3$ ... كما أن كون $x = 8$ و$y = 3$ هو ما يعطينا ما يُطلق عليه أصغر حل أساسي لمعادلة بِل $x^2 - 7y^2 = 1$. مع ذلك، فأحيانًا لا يظهر الحل الأساسي أبدًا في مرحلة مبكرة من المفكوك العشري؛ على سبيل المثال، أصغر حل موجب للمعادلة $x^2 - 29y^2 = 1$ هو $x = 9801$ و$y = 1820$. مع ذلك، فبمجرد تحديد هذا الحل الأساسي $(x, y)$، تظهر كل الحلول الأخرى عن طريق أخذ القوى المتتالية للتعبير الجبري $(x + y\sqrt{n})^k (k = 1, 2, 3, \ldots)$ واستخراج معاملات الأجزاء النسبية وغير النسبية المقابلة في مفكوك التعبير الجبري. وبهذه الطريقة نصل إلى مجموعة الحل الكامل لمعادلة بِل من خلال التمثيل الكسري المستمر للعدد $\sqrt{n}$.

الفصل الثامن

# الأعداد من منظور مختلف

## الأعداد الحقيقية والمركبة

إن تكوين الأعداد المركبة أكثر بساطة ويتم بسلاسة أكبر من تكوين الأعداد الحقيقية. فالمرحلة الأولى من تكوين الأعداد الحقيقية هي إنشاء الأعداد النسبية، وهي المرحلة التي ينبغي علينا فيها توضيح ما يعنيه الكسر. فالكسر — مثل $\frac{2}{3}$ — هو مجرد عددين صحيحين نعبِّر عنهما بهذه الطريقة المألوفة على الرغم من تميُّزها. وليس من الصعب فهْم فكرة الأجزاء الكسرية، مع أن الحسابات المتوافقة معها تتطلب جهدًا حثيثًا لإتقانها. وطالما شَرَحَ المعلمون لك في جملة أشياء أخرى أن كسورًا على غرار $\frac{2}{3}$ و$\frac{4}{6}$ و$\frac{6}{9}$ وما شابهها متساوية؛ ومع أنها لا تُمثِّل بالأزواج العددية نفسها، فإنها تمثل بالفعل أجزاءً متساوية. وهذا ليس أمرًا يصعب تقبُّله، ولكنه يلفت انتباهنا إلى حقيقة أن العدد النسبي هو في الواقع مجموعة لا متناهية من الكسور المتساوية التي يُمَثَّل كلٌّ منها بِزَوج من الأعداد الصحيحة. يبدو هذا مفزعًا، وربما نفضل ألا نفكر فيه كثيرًا؛ لأن احتمالية التلاعب بالمجموعات غير المتناهية التي تضم أزواجًا من الأعداد الصحيحة ربما تثير بعض القلق. ولكن هناك ميزة تنقذنا من ذلك؛ وهي أن أي كسر يمكن تمثيله تمثيلًا فريدًا ومختزلًا، يكون فيه البسط والمقام عددين أوليَّين، ويمكن الحصول عليهما من خلال التخلص من أي عوامل مشتركة في الكسر تكون قد بدأتْ بهما أولًا. ومع ذلك، بمجرد أن تعتاد على خصائص الكسور وقواعد استخدامها، ينبغي ألا تَحيد الأمور عن سياقها الصحيح، حتى لو أظهر الفحص الدقيق أنك تتلاعب ضمنًا بمجموعات لا متناهية تضم أزواجًا من الأعداد الصحيحة، بينما تجري عملياتك الحسابية.

مع ذلك، تسوء الأمور أكثر عند المرحلة التالية عند محاولة تحديد ماهية الأعداد الحقيقية حقًّا. دعنا نبدأ بمشكلة فيثاغورس؛ إذ اكتشف أنه لا يوجد كسر يساوي $\sqrt{2}$؛ لذا يمكننا تقديم رمز جديد $r$، ونمنحه خاصية $r^2 = 2$، ونكوِّن حقلًا جديدًا للأعداد من الأعداد النسبية والعدد الجديد $r$. وهذا فعَّال لأن مجموعة كل الأعداد التي تكون في صيغة $a + br$ — حيث $a$ و$b$ عددان نسبيان — تخضع لكل القواعد الجبرية العادية؛ فيمكننا حتى قِسْمتها؛ لأن مقلوب العدد من هذه الصيغة يحتفظ بصيغته، كما يمكن رؤيته من خلال مناورة جبرية بارعة يطلق عليها «ترشيد المقام».

يوفِّر العددان الجديدان $r$ و$-r$ حَلَّي المعادلة $x^2 = 2$، ولكن ماذا عن المعادلة $x^2 = 3$؟ يبدو أننا في حاجة لضم عدد جديد آخر من أجل حل هذه المعادلة؛ حيث إنه من اليسير التحقق من أنه لا يوجد عدد بصيغة $a + br$ سيكون ناتج تربيعه 3. (يكفي هنا الاستعانة ببرهان تناقُض بسيط: بافتراض أن $(a + br)^2 = 3$، فإن ذلك يسمح لك باستنتاج العبارة الجبرية الخاطئة التي تقول إن أحد العددين $\sqrt{2}$ أو $\sqrt{3}$ — على الأقل — نسبيٌّ بالرغم من كل شيء.)

إننا لَنرغب في تجاوُز كل هذه المخاوف حول معادلاتٍ بعينها، لِنعلن ببساطة أننا نعرف بالفعل ماهية الأعداد الحقيقية؛ فهي المجموعة التي تضم كل المفكوكات العشرية الممكنة، الموجبة والسالبة. وهذه الأعداد مألوفة للغاية، وإننا — بالممارسة — نعلم كيفية استخدامها؛ ومن ثم نشعر بأننا نقف على أرضية صلبة، على الأقل لِحِين طرح أسئلة أساسية للغاية. والسمة الرئيسية للأعداد هي إمكانية إجراء الجمع والطرح والضرب والقسمة عليها. ولكن على سبيل المثال، كيف يُفترض بك أن تضرب كسرين عشريين غير متكررين ولا متناهيين؟ إننا نعتمد على الكسور العشرية المتناهية لكي «نبدأ من النهاية اليمنى»، ولكن لا يوجد مثل هذا الأمر مع المفكوك العشري غير المتناهي. يمكن القيام بذلك، ولكنه أمر معقد للغاية نظريًّا وعمليًّا. إن نظام الأعداد الذي تعاني فيه من أجل توضيح كيفية الجمع والضرب لا يبدو مُرضيًا.

كما أن هناك عثرات صغيرة أخرى: عندما تضرب $\frac{1}{3}$ في 3، يكون الناتج 1. وعندما تضرب $0.333\ldots$ في 3، فإن الناتج بالتأكيد يكون $0.999\ldots$. وهي بالفعل الحالة التي يمكن أن يعبِّر فيها مفكوكان عشريان مختلفان عن العدد نفسه: $1.000\ldots = 0.999\ldots$. وفي الواقع، يحدث ذلك مع أي كسر عشري غير متكرر، على سبيل المثال: $0.375 = 0.374999\ldots$. ومن ثم، فإنه لا يمكن أن يكون من الصائب أبدًا قول إن

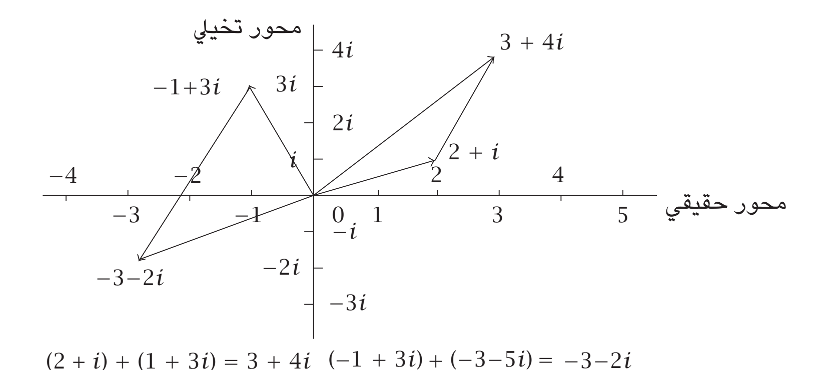
الكسور العشرية والأعداد الحقيقية تعبِّر كلٌّ منهما عن الأخرى؛ إذ نرى أن مفكوكين عشريين مختلفين يمكن أن يساويا العدد نفسه. علاوة على ذلك، سوف تتغير الأعداد ذات المفكوكات العشرية غير الفريدة، إذا عملنا على قاعدة أخرى غير القاعدة العشرية، وهذا يسبب تعقيدًا آخر. وإذا عرَّفنا الأعداد الحقيقية باستخدام الكسور العشرية، فإننا نجعل البنية تعتمد على خيار تعسفي (القاعدة العشرية). وإذا بَنَيْنا البنية نفسها في صورة ثنائية، فهل ستكون مجموعة «الأعداد الحقيقية» كما هي؟ وما الذي نعنيه بعبارة «كما هي» في أية حالة؟

قد تَجِدُ الأسئلةَ الأساسيةَ المُثارةَ أعلاه مثيرةً للاهتمام، أو قد تضيق ذرعًا بكل هذا التمحيص؛ إذ يبدو أننا نثير المتاعب لأنفسنا في حين كانت كل الأمور سابقًا تسير بسلاسة. مع ذلك، يوجد هدف جاد من وراء كل ذلك. فعلماء الرياضيات يدركون أنه كلما تُطرح أمور رياضية جديدة، فإنه من المهم تأسيسها على أمور رياضية معروفة، على سبيل المثال، بالطريقة التي يمكن من خلالها التفكير في الكسور على أنها زوج من الأعداد الصحيحة العادية. وبهذه الطريقة، ربما نضع بحذرٍ القواعدَ التي تَحْكم النظام الموسَّع الجديد، ونعرف وضْعنا الحالي. ولكن إذا تجاهَلْنا القواعد الأساسية تمامًا، فسوف تُلاحقنا فيما بعد. على سبيل المثال، أدى التطور السريع للتفاضل والتكامل — الذي نَتَج عن دراسة الحركة — إلى نتائج مذهلة مثل التنبؤ بحركة الكواكب. مع ذلك، فالتلاعب بالأمور غير المتناهية والتعامل معها على أنها متناهية قدَّم أحيانًا رؤًى مدهشة، وفي أوقات أخرى كان هراء. وبترسيخ الأنظمة الرياضية على أساس صلب يمكننا معرفة الفارق. وفي الواقع ينغمس علماء الرياضيات كثيرًا في تلاعبات «رسمية» من أجل معرفة إن كان استحداث بعض النظريات الجديدة الواعدة وشيكًا. وإذا كانت النتيجة جديرة بالاهتمام، فإنه يمكن إثباتها بدقة من خلال العودة للأساسيات، واللجوء إلى النتائج التي ثَبَتَت مصداقيتها سابقًا على نحو صحيح.

هذا هو السبب في تحمل يوليوس ديديكند (١٨٣١–١٩١٦) عناء وضْع نظام الأعداد الحقيقية رسميًّا، اعتمادًا على فكرته التي يشار إليها الآن باسم «حدود ديديكند» على خط الأعداد. مع ذلك، كان أول عالم رياضيات يتعامل بنجاح مع المعضلة التي سبَّبها وجود الأعداد غير النسبية هو يودوكسوس النيدوسي (بزغ نجمه عام ٣٨٠ قبل الميلاد) الذي سمحتْ «نظرية النِّسب» الخاصة به لأرخميدس باستخدام ما يطلق عليه «طريقة الاستنفاد» لدقة استنتاج مساحات وأحجام الأشكال المنحنية قبل ظهور علم التفاضل والتكامل بعد ذلك بقرابة ١٩٠٠ سنة.

## القطعة الأخيرة في أحجية الأعداد؛ الوحدة التخيلية

إنَّ إدخال رمز جديد $i$ يَنتج عن تربيعه $-1$ هو إجراء ناجح على نحو مذهل؛ إذ إنه لا يحل في لمح البصر مشكلة توفير حل لمعادلة واحدة فحسب، وإنما أيضًا يقدم حلًّا لكل المعادلات كثيرة الحدود، والكثير إلى جانب ذلك. وبالتأكيد، إنَّ لدينا جذرين تربيعيين لأي عدد سالب $-r$؛ حيث إن كلا العددين $\pm i\sqrt{r}$ يُربع إلى $-r$ بفضل خاصية أن $i^2 = -1$ وافتراض أن الضرب تبادلي — كما هي الحال مع العمليات الحسابية العادية — بمعنى أن $zw = wz$ لأي عددين $z$ و$w$. وبالفعل، إذا واصلْنا على أساس أن نظام الأعداد المركبة $a + bi$ يجب أن يشمل نظام الأعداد الحقيقية (وهو ما يتوافق مع الحالة التي يكون فيها $b = 0$)، وأنه يجب أن يستمر الالتزام بقواعد الجبر العادية، فلن تواجهنا صعوبات، وسنجد الكثير من المفاجآت السعيدة. إن مجموعة الأعداد المركبة التي يُرمز لها بالرمز $\mathbf{C}$ هي «حقل» يضمن أن القسمة ممكنة أيضًا ضمن أشياء أخرى. مع ذلك، فلمعرفة كيف يحدث ذلك كله، من الأفضل ترك أحادية خط الأعداد والنظر إلى الحياة من خلال بُعدين.




شكل ٨-١: إضافة الأعداد المركبة عن طريق إضافة قطع مستقيمة موجهة.

تقدم العمليات الحسابية للأعداد المركبة نفسها تقديمًا بارعًا على «المستوى المركب»؛ إذ نفكر في العدد المركب $a + bi$ بأنه يُمثَّل بالنقطة $(a, b)$ على المستوى الإحداثي.

وعندما نضيف العددين المركبين $z = (a, b)$ و$w = (c, d)$، فإننا نجمع مدخلاتهما الأولين معًا والثانيين معًا؛ لكي ينتج لدينا $z + w = (a + c, b + d)$. وإذا استخدمنا الرمز $i$، ينتج لدينا على سبيل المثال $(2 + i) + (1 + 3i) = 3 + 4i$.

وهذا يتوافق مع ما يُطلق عليه «جمع المتجهات» في المستوى المركب؛ حيث تُجمع القطع المستقيمة الموجهة («المتجهات») معًا، من الأعلى للأسفل (انظر شكل ٨-١). نبدأ من نقطة الأصل التي يكون إحداثيَّاها $(0, 0)$، وفي هذا المثال نرسم سهمنا الأول من هذه النقطة نحو النقطة $(2, 1)$. ولإضافة العدد الذي يمثَّل بالنقطة $(1, 3)$، نذهب للنقطة $(2, 1)$، ونرسم سهمًا يمثل التحرك وحدة واحدة لليمين في اتجاه أفقي (هذا هو اتجاه «المحور الحقيقي»)، وثلاثة وحدات لأعلى في اتجاه رأسي («المحور التخيلي»). فنصل إلى النقطة التي يكون إحداثيَّاها $(3, 4)$. ويمكننا — بالطريقة نفسها — أن نعرِّف طرح الأعداد المركبة عن طريق طرح الأجزاء الحقيقية والتخيلية بحيث نحصل على سبيل المثال على: $(11 + 7i) - (2 + 5i) = 9 + 2i$. ويمكن رسم ذلك عن طريق البدء من المتجه $(11, 7)$ وطرح المتجه $(2, 5)$، للانتهاء من الطرح وصولًا إلى النقطة $(9, 2)$.

أما الضرب، فهو موضوع آخر، ويسهل القيام به بصورة تقليدية؛ إذ نضرب العددَين المركَّبَين من خلال ضرب القوسَين معًا، متذكِّرين أن $i^2 = -1$. وبافتراض استمرار تطبيق «قانون التوزيع»، وهو قاعدة جبرية تسمح لنا بفك الأقواس بالطريقة العادية، فإن عملية الضرب تحدث كما يلي:

$$\begin{aligned}(a + bi)(c + di) &= a(c + di) + bi(c + di)\\ &= ac + adi + bci + bdi^2\\ &= (ac - bd) + (ad + bc)i\end{aligned}$$

على الجانب الآخر، يمكن حساب القسمة من خلال «المرافق المركب». فبوجه عام، المرافق $z = a + bi$ يرمز إليه بالرمز $\overline{z}$ وهو $a - bi$، بعبارة أخرى، $\overline{z}$ هو انعكاس $z$ على المحور الحقيقي. وقاعدة الضرب التي تطبق على $z\overline{z}$ ينتج عنها $a^2 + b^2$، وهو عدد حقيقي تمامًا كما يتضح أن الجزء التخيلي يبلغ صفرًا. وهذا يساوي مربع المسافة بين $z$ ونقطة الأصل، التي يشار إليها بالرمز $|z|$. ونعبر عن ذلك بالرموز كما يلي: $z\overline{z} = |z|^2$. وربما نقسم الآن عددًا مركبًا على آخر عن طريق ضرب الجزء العلوي والسفلي في مرافق

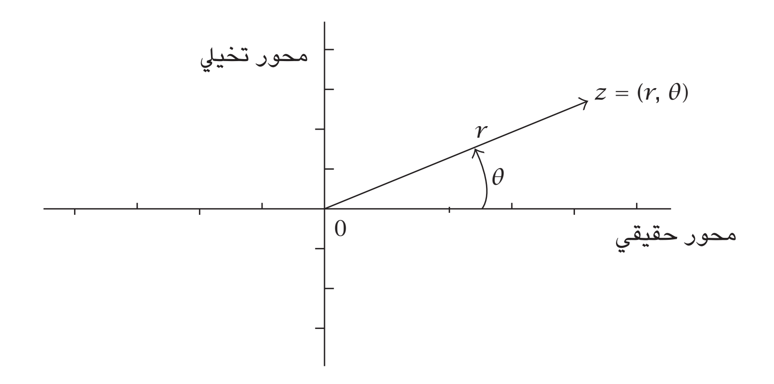
القاسم؛ لكي نجعل عملية القسمة تتم على عدد حقيقي على نحو خالص، وهذا يشبه الأسلوب المعياري لترشيد المقام الذي يُستخدم للتخلص من الجذور التربيعية في النتيجة النهائية، الذي استخدمناه في حساب الكسر المستمر للعدد $\sqrt{2}$. على سبيل المثال:

$$\frac{15+16i}{2+3i} = \frac{(15+16i)(2-3i)}{(2+3i)(2-3i)} = \frac{30-45i+32i-48i^2}{2^2-6i+6i-3^2i^2}$$
$$= \frac{(30+48)-(45-32)i}{2^2+3^2} = \frac{78-13i}{13} = 6-i.$$

عن طريق استخدام أعداد مركبة عامة بدلًا من الأعداد المركبة المحددة، يمكننا — بالطريقة نفسها — إيجاد نتيجة القسمة العامة للأعداد المركبة من حيث أجزاؤها الحقيقية والتخيلية، كما فعلنا آنفًا مع عملية ضرب الأعداد المركبة العامة. ومع ذلك، ما دام الأسلوب مفهومًا، فلا توجد حاجة مُلحَّة لإنتاج وحفظ الصيغة الناتجة.

ولعملية الضرب تفسيرٌ هندسي يَظهر إذا غَيَّرْنا نظامنا الإحداثي من الإحداثيات الكارتيزية العادية إلى إحداثيات قطبية. في هذا النظام تُحدد النقطة $z$ مرة أخرى عن طريق زوج مرتب من الأعداد، الذي سنعبر عنه كالآتي $(r,\theta)$. العدد $r$ هو «المسافة» التي تبعدها نقطتنا $z$ عن نقطة الأصل $O$ (يطلق عليها في هذا السياق اسم «قطب»). لذا، فـ $r$ كمية غير سالبة، وكل النقاط التي تحمل قيمة $r$ نفسها تشكل دائرة نصف قطرها $r$ متمركزة عند القطب. ونستخدم الإحداثي الثاني $\theta$ لتحديد $z$ على هذه الدائرة عن طريق اعتبار $\theta$ الزاوية، وتقاس في اتجاه عكس اتجاه عقارب الساعة، من المحور الحقيقي إلى الخط $Oz$. ويُطلق على العدد $r$ «مقياس» $z$، بينما يطلق على الزاوية $\theta$ «البعد الزاوي» لـ $z$.

افترض الآن أن لدينا عددين مركبين $z$ و$w$، إحداثياتهما القطبية $(r_1,\theta_1)$ و$(r_2,\theta_2)$ على الترتيب، فيتضح أن الإحداثيات القطبية للناتج $zw$ تأخذ صورة بسيطة وظريفة. ويمكن التعبير عن قاعدة التركيب على نحو منظم بلغة عادية على النحو الآتي: مقياس الناتج $zw$ هو حاصل ضرب مقياس كلٍّ من $z$ و$w$، بينما البعد الزاوي $zw$ هو مجموع البعد الزاوي لكلٍّ من $z$ و$w$. وبالرموز، للعدد $zw$ إحداثيات قطبية $(r_1r_2,\theta_1+\theta_2)$. تتدرج عملية ضرب الأعداد الحقيقية تحت هذه الطريقة الأكثر عمومية للنظر للأشياء؛ على سبيل المثال، العدد الحقيقي الموجب $r$ له الإحداثيات القطبية $(r,0)$، وإذا ضربناه في إحداثيات عدد آخر $(s,0)$، فإن النتيجة تكون هي النتيجة المتوقعة $(rs,0)$، المتوافقة مع العدد الحقيقي $rs$.




شكل ٨-٢: موضع عدد مركب على الإحداثيات القطبية.

يتكشف المزيد من سمات ضرب الأعداد المركبة من خلال هذا التمثيل. وتتحدد الإحداثيات القطبية للوحدة المركبة $i$ من خلال $(1, 90°)$. (وفي العادة، لا تقاس الزوايا بالدرجات في هذه الظروف، ولكن بالوحدة الرياضية الطبيعية «راديان»: يبلغ مقدار قياس زاوية الدائرة $2\pi$ راديان؛ حيث إن لفة الراديان الواحد تضاهي التحرك بمقدار وحدة واحدة على محيط الدائرة الوحدة، بالارتكاز على نقطة الأصل. والراديان الواحد يساوي تقريبًا $57.3°$.) وإذا أخذنا الآن أي عدد مركب $z = (r, \theta)$ وضربناه في $i = (1, 90°)$، نجد أن $zi = (r, \theta + 90°)$. وهذا يعني أن «الضرب في $i$ يضاهي الدوران خلال زاوية قائمة حول مركز المستوى المركب». بعبارة أخرى، الزاوية القائمة — هذه الفكرة الهندسية الأساسية — يمكن تمثيلها كعدد.

في الواقع، إنَّ تأثير الجمع أو الضرب في العدد المركب $z$ على كل النقاط في مساحة محددة على المستوى المركب يمكن تصويره هندسيًّا. تَصوَّرْ أي مساحة تتخيلها على المستوى، إذا جَمَعْنا $z$ مع كل نقطة داخل المساحة، فإننا ببساطةٍ نحرك كلَّ نقطةٍ المسافةَ نفسها في الاتجاه نفسه الذي يحدده السهم — أو المُتجَه كما نطلق عليه غالبًا — ممثَّلًا بـ $z$. بمعنى أننا ننقل المساحة إلى موضع آخر على المستوى، بحيث يُحافَظ على الشكل والحجم كما هما، وكذلك وضعها، ونعني بهذا أن المساحة لا تتعرض لأي دوران أو انعكاس. مع ذلك، فإن ضرب كل نقطة في منطقتك في $z = (r, \theta)$ له أثران، يتسبب $r$ في أحدهما ويتسبب $\theta$ في الآخر. ويزداد مقياس كل نقطة في المساحة بعامل $r$، وبهذا

تزداد كل أبعاد المساحة بعامل $r$ أيضًا (وبهذا تُضرب مساحتها في عامل $r^2$). وبالطبع، إذا كان $r < 1$، فإن هذا التوسع يوصف على نحو أفضل كَانْكِمَاش؛ إذ إن المساحة الجديدة سوف تكون أصغر من المساحة الأصلية. مع ذلك، فسوف تحافظ المساحة على شكلها؛ على سبيل المثال، يُنقل المثلث إلى مثلث مشابه له الزوايا نفسها كسابقه. أما تأثير $\theta$ — كما أوضحنا آنفًا — فهو تدوير المساحة من خلال زاوية $\theta$، في اتجاه عكس عقارب الساعة حول القطب. والتأثير الإجمالي إذن لضرب كل نقاط منطقتك في $z$ هو توسيع وتدوير منطقتك حول القطب. وسوف تظل المساحة الجديدة محتفظة بالشكل نفسه كما كانت، ولكن سيختلف حجمها الذي سيحدده $r$، وسوف يختلف وضعها كما ستحدده زاوية التدوير $\theta$.

## نتائج أخرى

إن النسخة القطبية من الأعداد المركبة مناسبة على نحو خاص لأخذ القوى والجذور لرفع $z = (r, \theta)$ للقوة الموجبة $n$. فببساطة نرفع المعامل لهذه القوة ونضاعف $\theta$ عدد $n$ من المرات؛ لنحصل على $z^n = (r^n, n\theta)$. وتنطبق الصيغة نفسها على القوى الكسرية والسالبة. ويمكن فهم القسمة أيضًا بالصورة القطبية. فكما هي الحال مع الأعداد الحقيقية، القسمة على عدد مركب $z$ تعني الضرب في مقلوبه $w = \frac{1}{z}$، ولكن ما هذا العدد $w$؟ بفرض أن $z = (r, \theta)$ فإن العدد $w$ هو العدد الذي له خاصية $zw = (1, 0)$، وهو العدد 1. وهذا يوضح لنا أنه يجب أن يكون $w = (\frac{1}{r}, -\theta)$؛ لكي يكون حينها $zw = (r, \theta)(\frac{1}{r}, -\theta) = (r\frac{1}{r}, \theta - \theta) = (1, 0)$، كما نريد. وهذا يوفر بديلًا للمنهج الكارتيزي في القسمة الذي يستخدم المرافقات المركبة.

يوجد عدد كبير من تطبيقات الأعداد المركبة، حتى على المستوى الأوَّلي؛ فالتفاعل بين التمثيلات الكارتيزية والقطبية يحفِّز استخدام حساب المثلثات بطريقة مدهشة ومفيدة. على سبيل المثال، التمرين العادي للطلاب هو اشتقاق المتطابقات المهمة التي تظهر الآن بتلقائية شديدة عن طريق استخراج أعداد مركبة اعتباطية من معامل الوحدات (مثل $r = 1$)، ثم حساب القوى باستخدام الإحداثيات الكارتيزية ثم القطبية. ووضع معادلة لصورتَي الإجابة يكشف حينها عن معادلة نِسب مثلثية.

إنَّ النقطة ذات الإحداثيين القطبيين $(1, \theta)$ لها — من خلال أساسيات حساب المثلثات — الإحداثيان الكارتيزيان $(\cos\theta, \sin\theta)$. وإذا ضربنا الآن هذين العددين

المركبين $z = \cos\theta + i\sin\theta$ و$w = \cos\phi + i\sin\phi$ في الإحداثيات الكارتيزية، نحصل على:

$$zw = (\cos\theta\cos\phi - \sin\theta\sin\phi) + i(\cos\theta\sin\phi + \sin\theta\cos\phi);$$

بينما ينتج عن العملية نفسها في الإحداثيات القطبية:

$$zw = (1, \theta)(1, \phi) = (1, \theta + \phi) = \cos(\theta + \phi) + i\sin(\theta + \phi);$$

حيث إن معادلة الأجزاء الحقيقية والتخيلية لنسختَيْ هذا الناتج الواحد تُنتج بسهولة صيغَ حساب المثلثات لمجموع قياس الزاوية المعيارية:

$$\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi,$$

$$\sin(\theta + \phi) = \cos\theta\sin\phi + \sin\theta\cos\phi.$$

بدلًا من ذلك، يمكن اشتقاق النسخة القطبية للضرب المركب باستخدام هذه الصيغ الخاصة بحساب المثلثات. وفي الواقع، القاعدة التي ذكرناها هنا — دون برهان — للضرب في النسخة القطبية عادةً ما تُشتق أولًا من الصورة الكارتيزية عن طريق استخدام صيغ حساب المثلثات.

يَحدث ما هو أكثر من ذلك بسهولة شديدة في الوقت الحالي؛ لأن استخدام الأعداد المركبة يكشف عن رابط بين الدالة الأسية أو الدالة ذات القوة الجبرية، والدوال المثلثية التي تبدو ظاهريًّا غير ذات صلة. فدون المرور من البوابة التي يقدمها الجذر التربيعي لسالب واحد، ربما يمكن لمح الرابط دون فهْمه. وتنشأ الدالة التي يطلَق عليها «الدالة الزائدية» من أَخْذ ما يُعرف بأنه الأجزاء الزوجية والفردية للدالة الأسية؛ إذ يتوافق مع كل متطابقة مثلثية متطابقة أخرى شبيهة بها، ولكن ربما باستثناء العلامة، بما في ذلك هذه الدوال المثلثية الزائدية. ويمكن التحقق من صحة ذلك بسهولة في أي حالة محددة، ولكن حينها سيظل السؤال مطروحًا: لماذا يحدث ذلك من الأساس؟ لماذا ينبغي أن ينعكس سلوك فئة من الدوال انعكاسًا دقيقًا على فئة أخرى، ويتضح بهذا الأسلوب المختلف للغاية ويتسم بهذه السمة المختلفة؟ يُحل هذا اللغز عن طريق الصيغة $e^{i\theta} = \cos\theta + i\sin\theta$، التي توضح أن الدوال الأسية والدوال المثلثية ترتبط ارتباطًا

وثيقًا كلٌّ منها بالأخرى، ولكن فقط عن طريق استخدام الوحدة التخيلية $i$. وبمجرد الكشف عن ذلك (لأنه مفاجئ وليس بديهيًّا على الإطلاق)، يصبح من الواضح أن النتائج المذكورة حتمية عن طريق أداء الحسابات باستخدام التمثيلَين البديلين اللذين تقدمهما هذه المعادلة، ثم المعادلة بين الأجزاء الحقيقية والتخيلية. مع ذلك، فدون الصيغة يبقى الأمر كله لغزًا.

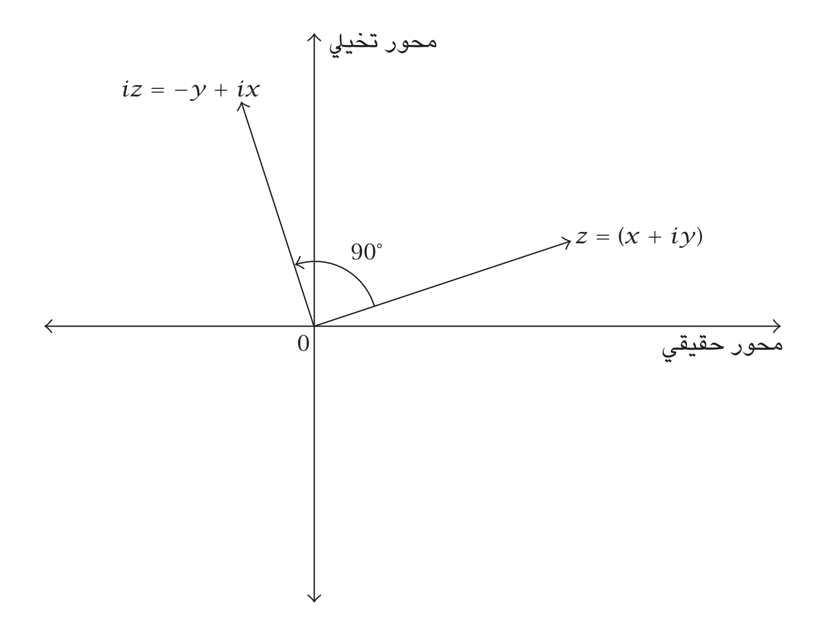
## الأعداد المركبة والمصفوفات

دعنا ندقق النظر في بعض نتائج اكتشاف أن الضرب في $i$ يمثل دورانًا بمقدار زاوية قائمة حول مركز المستوى الإحداثي. إذا كان $z = x + iy$، إذن فإنه يكون لدينا من خلال فك الأقواس وإعادة ترتيب عمليات الضرب $i(x + iy) = -y + ix$، بحيث تنتقل النقطة $(x, y)$ بسبب هذا التدوير إلى $(-y, x)$؛ انظر شكل ٨-٣. وبهذه الطريقة، يمكن اعتبار أن الضرب في $i$ أُجري على النقاط في المستوى. ويتمتع هذا الإجراء بسمة خاصة، وهي أنه بالنسبة لأي نقطتين $z$ و$w$ وأي عدد حقيقي $a$، يكون لدينا $i(z + w) = iz + iw$، و$i(aw) = a(iw)$.

علاوة على ذلك، إذا ضربنا عددًا حقيقيًّا $a$ في عدد مركب $x + iy$، نحصل على $a(x + iy) = ax + i(ay)$. وفيما يتعلق بالنقاط على المستوى المركب، تُنقل $(x, y)$ إلى $(ax, ay)$، أو تكتب بطريقة أخرى: $a(x, y) = (ax, ay)$.

تُعرف أنواع العمليات التي تتمتع بهاتين السمتين بأنها «خطية» ولها أهمية قصوى في جوانب الرياضيات كلها. وهنا أتمنى فقط أن أَلْفِتَ انتباهك إلى حقيقة أن تأثير هذه العملية $L$ يحدده عملها على النقطتين $(1, 0)$ و$(0, 1)$، ولهذا دعنا نفترض أن $L(1, 0) = (a, b)$ و$L(0, 1) = (c, d)$. ولهذا، فإنه لأي نقطة $(x, y)$، سيكون لدينا $(x, y) = x(1, 0) + y(0, 1)$؛ ومن ثم فباستخدام العمليات الخطية، نحصل على:

$$\begin{aligned} L(x, y) &= L(x(1, 0) + y(0, 1)) = xL(1, 0) + yL(0, 1) \\ &= x(a, b) + y(c, d) = (ax, bx) + (cy, dy) \\ &= (ax + cy, bx + dy). \end{aligned}$$




شكل ٨-٣: الضرب في $i$ يعمل على دوران العدد المركب بمقدار زاوية قائمة.

ربما تُختصر هذه المعلومة عن طريق ما يطلق عليه «معادلة مصفوفية»:

$$(x, y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (ax + cy, bx + dy).$$

ذكرنا هنا مثالًا على ضرب المصفوفات، الذي يوضح طريقة تنفيذ هذا الإجراء بوجه عام. و«المصفوفة» ما هي إلا نسق مستطيل من صفوف وأعمدة من الأعداد. مع ذلك، تمثل المصفوفات نوعًا آخر من العناصر العددية ثنائية الأبعاد، وأكثر من ذلك أنها تتخلل تقريبًا كل فروع الرياضيات المتقدمة، سواء البحتة أو التطبيقية؛ فهي تمثل أساس الجبر، ويسعى قدر كبير من الرياضيات الحديثة لتمثيل نفسه عن طريق المصفوفات، وذلك لفائدتها التي ثبتت بالبرهان. ويمكن جمْع مصفوفتين تتضمنان العدد نفسه من الأعمدة والصفوف معًا — كل مدخل مع الآخر — على سبيل المثال، للتوصل إلى

مدخل الصف الثاني والعمود الثالث في مجموع المصفوفتين، نجمع فحسب المدخلين الموجودين في الموقعين المقابلين في المصفوفتين المَعْنيَّتين. غير أن ضرْب المصفوفات يمنح الموضوع سمة جديدة ومهمة، وطريقة تنفيذ هذه العملية ظهرتْ من تلقاء نفسها في المثال السابق؛ إذ يتكون كل مدخل في المصفوفة الناتجة عن طريق أخذ المضروب العددي لصف من المصفوفة الأولى مع عمود من المصفوفة الثانية؛ مما يعني أن يكون المدخل مجموع النواتج المتماثلة عند وضع صف المصفوفة الأولى أعلى عمود المصفوفة الثانية.

تتبع المصفوفات كل قوانين الجبر العادية عدا تبادلية الضرب؛ بمعنى أنه بالنسبة للمصفوفتين $A$ و$B$ ليس صحيحًا بوجه عام أن تكون $AB = BA$. مع ذلك، فإن ضرب المصفوفات يمثل عملية تجميع؛ بمعنى أن نواتج أي نطاق تُكتب على نحو لا لبس فيه دون الحاجة إلى وضع أقواس.

تُعد التحولات الخطية على المستوى — نموذجيًّا — دورانًا حول نقطة الأصل، وانعكاسات في الخطوط عبر نقطة الأصل، وتوسعات وانكماشات حول نقطة الأصل؛ ومن ثم يُطلَق عليها «المقصات» (أو الخطوط المائلة)، التي تحرِّك النقاط بالتوازي إلى محور ثابت بقدر يتناسب مع بُعدها عن هذا المحور بطريقة تشبه تقليب صفحات الكتاب صفحة وراء الأخرى. وأيُّ تسلسل من هذه التحولات يمكن أن يتأثر بضرب كل المصفوفات ذات الصلة معًا للحصول على مصفوفة واحدة لها التأثير النهائي نفسه؛ إذ تعمل كل هذه التحولات بالترتيب. وصفوف المصفوفة الناتجة تكون ببساطة صورًا للنقطتين $(1,0)$ و$(0,1)$، كما رأينا آنفًا، تُعرف باسم «متجهات الأساس».

من الطبيعي الآن الالتفات إلى المصفوفة $J$ التي تمثل دورانًا عكس عقارب الساعة بمقدار زاوية قائمة حول نقطة الأصل؛ إذ يجب أن تحاكي السلوك الذي شهدناه عند الضرب في الوحدة التخيلية $i$. نظرًا لأن النقطة $(1,0)$ انتقلت للنقطة $(0,1)$ عن طريق التدوير، وعلى نحو مشابه انتقلت النقطة $(1,0)$ إلى $(-1,0)$، فإن هذين المتجهين يشكلان صفوف مصفوفتنا $J$. ونتيجة تربيع المصفوفة $J$ سوف تكون مصفوفة لها التأثير الهندسي لنقاط التدوير بمقدار $2 \times 90^\circ = 180^\circ$ حول نقطة الأصل. وتم حساب ذلك أسفله عن طريق ضرب المصفوفة. على سبيل المثال، لمعرفة المدخل الأخير ناحية اليمين في المصفوفة $J^2$، نأخذ المضروب العددي للصف الثاني والعمود الثاني، الذي

يكون $-1 = 0 + 1- = 0 \times 0 + 1 \times (-1)$. والحساب الكامل يتضمن الناتج التالي:

$$J^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I.$$

تمثل المصفوفة $I$ ذات الصفوف (10) و(01) المصفوفة المحايدة، وتسمى بهذا؛ لأنها تعمل كالعدد 1؛ إذ إنها عند ضربها في مصفوفة أخرى $A$، فإن النتيجة تكون $A$. أما المصفوفة $-I$، التي تمثل دورانًا يعادل نصف لفة كاملة حول نقطة الأصل، فإنها تتصرف مثل $-1$ في أن $(-I)^2 = I$. ونتيجة كل هذا هو أن المصفوفات $aI + bJ$ — حيث $a$ و$b$ عددان حقيقيان — تحاكي بدقة الأعداد المركبة $a + bi$ فيما يخص الجمع والضرب؛ ومن ثم تقدم تمثيلًا مصفوفيًّا لحقل العدد المركب. والمصفوفة المقابلة للعدد المركب النموذجي $a + bi$ هي:

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

تتبادل المصفوفاتُ التي تمثِّل الأعداد المركبة بالفعل بعضُها مع بعض، ولكن — كما ذكرنا آنفًا — لا ينطبق كل هذا عمومًا على كل نواتج المصفوفات، والطريقة الأخرى التي يمكن للمصفوفات بها أن تتصرف على نحو غير مألوف هي أنها لا يمكن عكسها جميعًا. وبالنسبة لكل المصفوفات المربعة $A$ (وهي المصفوفة التي تحتوي على العدد نفسه من الصفوف والأعمدة)، ربما نجد «مصفوفة معكوسة» $B$ فريدة من نوعها، يكون فيها $AB = BA = I$؛ أي تكون مصفوفة محايدة. مع ذلك، يعتمد وجود المصفوفة المعكوسة على عدد واحد يقترن بالمصفوفة المربعة يُعرف باسم «المحدِّد». وبوجه عام، يمثل هذا العدد مجموع نواتج مؤشَّر عليها تتكون عن طريق أَخْذ مدخل واحد من كل صف وعمود من نسق المصفوفة. وبالنسبة لنسق المصفوفة العادية المكونة من صفين وعمودين — كما ذكرنا آنفًا — فإن المحدِّد هو العدد $\Delta = ad - bc$. وللمحدداتِ الكثيرُ من الاستخدامات والسمات المستحسنة؛ فعلى سبيل المثال، يمثل $\Delta$ مقياس المساحة لتحوُّل المصفوفة المقابلة: شكل المساحة $a$ سوف يتحول إلى شكل المساحة $\Delta a$ عندما يتحول بفعل هذه المصفوفة (وإذا كانت $\Delta$ سالبة، فإن الشكل يخضع أيضًا لعملية

انعكاس؛ إذ ينعكس الاتجاه الأصلي). علاوة على ذلك، إنَّ محدِّد حاصل ضرب مصفوفتين مربعتين هو حاصل ضرب محددات هاتين المصفوفتين. والمصفوفة المربعة $A$ سيكون لها مصفوفة معكوسة $B$ إلا في حالة $\Delta = 0$، التي لن يكون للمصفوفة فيها معكوسٌ أبدًا. فالمحدِّد الذي يبلغ صفرًا يقابل هندسيًّا تحولًا اضمحلاليًّا تنهار فيه مساحات المصفوفة وتتحول إلى مساحات صفرية كقطعة مستقيمة أو حتى نقطة وحيدة.

في مصفوفة العدد المركب $z = a + bi$، نلاحظ أن $\Delta = a^2 + b^2$، الذي لا يكون صفرًا أبدًا إلا عندما $z = 0$؛ ولكن بالطبع لم يكن للصفر مقلوب من قبل، ولا تزال تلك هي الحال في الميدان الأوسع للأعداد المركبة. ولكن هذا يؤكد بالفعل أن كل عدد مركب ليس صفرًا يمتلك معكوسًا ضربيًّا.

نقف هنا على حافة العوالم الشاسعة التي تضم الجبر الخطي ونظرية التمثيل وتطبيقات التفاضل والتكامل متعددة الأبعاد، ولكن لا يمكن التعمق في هذه العوالم الآن. مع ذلك ينبغي للقارئ أن يدرك أن المصفوفات تنطبق على مساحات ثلاثية الأبعاد، وفي الواقع على مساحات ذات الأبعاد $n$، عادة من خلال المصفوفات $n \times n$. ومع أن نسق المصفوفات يصبح أكبر وأكثر تعقيدًا، فإن المصفوفات نفسها تظل كيانات عددية ثنائية الأبعاد.

## أعداد فيما وراء المستوى المركب

إن حقل $\mathbf{C}$ الذي يتضمن الأعداد المركبة جميعها يُعتبر «متكاملًا» بطريقتين مهمتين؛ إذ يُطلق على أي متتالية لا متناهية من الأعداد المركبة — التي تتجمع فيها الحدود في دوائر أصغر حجمًا ذات نصف قطر يصل إلى الصفر — اسم متتالية «متقاربة»؛ وأي متتالية متقاربة تضم أعدادًا مركبة تصل إلى عدد مركب متناهٍ. وهذا أيضًا ينطبق على الأعداد الحقيقية، ولكنه لا ينطبق على الأعداد النسبية؛ فالتقريب العشري المتتابع لأي عدد غير نسبي يمثل متتالية من الأعداد النسبية التي تصل إلى حد خارج نطاق الأعداد النسبية. علاوة على ذلك، يُعد الحقل $\mathbf{C}$ متكاملًا (أو مغلقًا) من الناحية الجبرية؛ حيث يمكن توضيح أن أي معادلة كثيرة الحدود $p(z) = a + bz + cz^2 + \cdots + z^n = 0$ لها $n$ من الحلول (المركبة) — $z_1, z_2, \ldots, z_n$ — تسمح حينها للطرف $p(z)$ نفسه أن يتحلل بالكامل إلى عوامل $p(z) = (z - z_1)(z - z_2)\ldots(z - z_n)$.

وهذا الأمر والنجاحات المذهلة الأخرى للأعداد المركبة تُغني إلى حد كبير عن الحاجة لتوسيع نطاق نظام الأعداد لما يتجاوز المستوى المركب. وفي الواقع ليس من الممكن بناء

نظام أعداد موسع يتضمن C ويحتفظ أيضًا بكل قوانين الجبر العادية. علاوة على ذلك، يوجد فقط نظامان موسعان يحتفظان بالكثير من البنية الجبرية، وهما «الكواتيرنيون» و«الأوكتونيون». ومع أن استخدامهما ليس منتشرًا تقريبًا بنفس قدر انتشار الأعداد المركبة، فإن الكواتيرنيون يُستخدم — على سبيل المثال — في رسومات الكمبيوتر ثلاثية الأبعاد. أما الأوكتونيون — الذي يمكن اعتباره زوجًا من الكواتيرنيون — فلا يفتقر فقط إلى سمة التبادلية، وإنما يفتقر أيضًا إلى سمة التجميعية الخاصة بعملية الضرب.

الكواتيرنيون هو عدد بصيغة $z = a + bi + cj + dk$؛ حيث يكون الجزء الأول $a + bi$ عددًا مركبًا عاديًّا، ووحدتا الكواتيرنيون $j$ و$k$ تستوفيان الشرط $j^2 = k^2 = -1$. ولكي نجري عمليات الضرب في الكواتيرنيون، يلزم أن نعلم طريقة ضرب الوحدات بعضها في بعض، ويتحدَّد ذلك وفق القواعد $ij = k, jk = i, ki = j$، ولكن الناتج المعكوس يحمل العلامة المعكوسة، بحيث يكون على سبيل المثال: $ji = -k$ (وربما تُشتق كل هذه النواتج في الواقع من معادلة إضافية واحدة: $ijk = -1$). وبذلك، يشكل الكواتيرنيون نظامًا جبريًّا متقدمًا يستوفي كل قوانين الجبر باستثناء تبادلية الضرب، بسبب تغيرات العلامة المذكورة سابقًا في النواتج المعكوسة. وكذلك يمكن إيضاح اتساق النظام من خلال تمثيل المصفوفات المكونة من عمودين وصفَّين، ولكن هذه المرة نسمح بوجود العناصر المركبة لا مدخلات الأعداد الحقيقية فقط. ويرتبط العدد 1 مرة أخرى بالمصفوفة المحايدة $I$، ولكن يكون للوحدات $i$ و$j$ و$k$ نظراؤها في المصفوفة:

$$i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

في حين يكون للكواتيرنيون العادي $z$ مصفوفته الخاصة:

$$z = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

مع ذلك، فليس تمثيل الكواتيرنيون بالمصفوفات فريدًا من نوعه، ولكن لتمثيل الأعداد المركبة بمصفوفات بدائل مكافئة أيضًا بالفعل. علاوةً على ذلك، من الممكن تمثيل الكواتيرنيون دون استخدام الأعداد المركبة، ولكن فقط على حساب استخدام نسق

مصفوفات أكبر؛ فالكواتيرنيون يمكن تمثيلها بمصفوفات معينة ذات أربعة صفوف وأعمدة بمدخلات من الأعداد الحقيقية فحسب.

ظهرت أنواع جديدة من الأعداد، وكذلك التوسعات في الأنظمة القديمة؛ بسبب الحاجة لأداء عمليات حسابية لم يكن من الممكن الوصول إلى نتائجها باستخدام نظام الأعداد كما هو. وكل حضارة تبدأ بأعداد العد، ولكن العمليات الحسابية التي تتضمن الأجزاء تؤدي إلى الكسور، والتي تتضمن الديون تؤدي إلى الأعداد السالبة، وكما اكتشف فيثاغورس، تؤدي تلك التي تتضمن الأطوال إلى الأعداد غير النسبية. ومع قِدَم اكتشاف حقيقة أنه لا يمكن التعامل مع كل الأمور العددية باستخدام الأعداد الصحيحة ونسبها، فإن هذا الاكتشاف كان دقيقًا على نحو أعمق من كل ذلك. فعندما أصبحت العلوم أكثر تقدمًا، لزم أن تنضج أنظمة الأعداد لكي تتوافق مع هذا التقدم. ولا يتطلع العلماء بوجه عام إلى إنشاء نظم أعداد جديدة بطريقة شاذة يصعب التنبؤ بها. بل على العكس من ذلك، تُقَدَّم هذه الأنظمة في كثير من الأحيان على مَضَض وبتردُّدٍ في البداية للتعامل مع المسائل البحثية. على سبيل المثال، رغم عرض المصفوفات لأول مرة في القرن التاسع عشر، فإنها ظهرت على نحو لا يُقاوم في ميكانيكا الكم في بدايات القرن العشرين عندما واجه علماء الفيزياء كمية بصيغة $q = AB - BA$ لم تبلغ صفرًا مع ذلك. وفي أي نظام أعداد يتسم بالتبادلية كانت $q$ تبلغ صفرًا بالطبع؛ لذا لم تكن الكيانات العددية اللازمة هنا كالكيانات التي صادفوها من قبل، بل كانت مصفوفات.

يبدو الآن أن عالَم الرياضيات والفيزياء لديه أنواع كافية من الأعداد؛ ومع وجود أنواع لم تُذكَر هنا في هذا الكتاب، فإن الأنواع التي تُستخدَم على نحو شائع في الرياضيات والعلوم لم يلزم تغييرها بقدر كبير منذ النصف الأول من القرن العشرين.

مع ذلك، فَبِوُصولنا لهذه الملاحظات نكون قد وَصَلْنا إلى نهاية رحلتنا في عالم الرياضيات، بعد أن بدأْنا الرحلة بالمستوى التمهيدي وتدرَّجْنا صعودًا إلى أعلى حيث آمل أن يلقي القارئ نظرة على عالم الأعداد الثري والغامض.

# قراءات إضافية

Two other books in the OUP VSI series that complement and expand on the current one are *Mathematics* by the Field's medallist Timothy Gowers and *Cryptography* by Fred Piper and Sean Murphy. Probability and statistics, fields that were neglected here in *Numbers*, are the subject of the *VSI Statistics* by David J. Hand.

An insight into the nature of numbers can be read in David Flannery's book, *The Square Root of 2: A Dialogue Concerning a Number and a Sequence* (Copernicus Books, 2006). This leisurely account is in the Socratic mode of a conversation between a teacher and pupil. *One to Nine: The Inner Life of Numbers* by Andrew Hodges (Short Books, 2007) analyses the significance of the first nine digits in order. Actually it uses each number as an umbrella for examining certain fundamental aspects of the world and introduces the reader to all manner of deep ideas. This contrasts with Tony Crilly's *50 Mathematical Ideas You Really Need To Know* (Quercus Publishing, 2007), which does as it says, digesting each of 50 notions into a four-page description in as straightforward a manner as possible. The explanations are mainly through example with a modest amount of algebraic manipulations involved, rounded off with historical details and timelines surrounding the commentary. A particularly nice

account on matters concerned with binomial coefficients is the paperback of Martin Griffiths, *The Backbone of Pascal's Triangle* (UK Mathematics Trust, 2007), in which you will read proofs of Bertrand's Postulate and Chebyshev's Theorem, giving bounds for the number of primes less than $n$.

*Elementary Number Theory* by G. and J. Jones (Springer-Verlag, 1998) gives a gentle but rigorous introduction and goes as far as aspects of the famous Riemann Zeta Function and Fermat's Last Theorem. The classic book *An Introduction to the Theory of Numbers*, by G. H. Hardy and E. M. Wright, 6th edn (Oxford University Press, 2008) assumes little particular mathematical knowledge but hits the ground running. The author's book *Number Story: From Counting to Cryptography* (Copernicus Books, 2008) has more in the way of the history of numbers than this *VSI* and includes mathematical details in the final chapter. *The Book of Numbers* by John Conway and Richard Guy (Springer-Verlag, 1996) is full of history, vivid pictures, and all manner of facts about numbers. Quite a lot of the history and mystery surrounding complex numbers is to be found in *An Imaginary Tale: The Story of* $\sqrt{-1}$ (Princeton University Press, 1998) by Paul J. Nahin. Paul Halmos's *Naive Set Theory* (Springer-Verlag, 1974) gives a quick mathematical introduction to infinite cardinal and ordinal numbers, which were not introduced here.

A popular account of the Riemann Zeta Function is the book by Marcus du Sautoy, *The Music of the Primes, Why an Unsolved Problem in Mathematics Matters* (HarperCollins, 2004), while Carl Sabbagh's, *Dr Riemann's Zeros* (Atlantic Books, 2003) treats essentially the same topic.

There are two accounts of the solution to Fermat's Last Theorem, those being *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem* by Amir D. Aczel (Penguin, 1996) and *Fermat's Last*

*Theorem* by Simon Singh (Fourth Estate, 1999). The best popular book on the history of coding up to the RSA cipher is also an effort of Simon Singh: *The Code Book* (Fourth Estate, 2000). The unsolvability of the quintic (fifth-degree polynomial equations) was not explained in our text here but is the subject of an historical account: *Abel's Proof: An Essay on the Sources and Meaning of Mathematical Unsolvability* (MIT Press, 2003) by Peter Pesic.

## مواقع ويب

A very high-quality web page that allows you to dip into any mathematical topic, and is especially rich in number matters, is Eric Wolfram's *MathWorld: mathworld.wolfram.com*. For mathematical history topics, try *The MacTutor History of Mathematics archive* at St Andrews University, Scotland: *https://www-history.mcs.st-andrews.ac.uk/history.index.html*. Web pages accessed 8 October 2010. Wikipedia's treatment of mathematics by topic is generally serious and of good quality, although the degree of difficulty of the treatments is a little variable. For example, Wikipedia gives a good quick overview of important topics such as matrices and linear algebra.